AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

LEGISLATING TO STOP THE ONSLAUGHT OF ANNOYING ROBOCALLS

HEARING

BEFORE THE

SUBCOMMITTEE ON COMMUNICATIONS AND TECHNOLOGY

OF THE

COMMITTEE ON ENERGY AND COMMERCE
HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTEENTH CONGRESS

FIRST SESSION

APRIL 30, 2019

Serial No. 116–26

Printed for the use of the Committee on Energy and Commerce
govinfo.gov/committee/house-energy
energycommerce.house.gov

U.S. GOVERNMENT PUBLISHING OFFICE
39–858 PDF WASHINGTON : 2020

COMMITTEE ON ENERGY AND COMMERCE

FRANK PALLONE, JR., New Jersey
Chairman

BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
ELIOT L. ENGEL, New York
DIANA DEGETTE, Colorado
MIKE DOYLE, Pennsylvania
JAN SCHAKOWSKY, Illinois
G. K. BUTTERFIELD, North Carolina
DORIS O. MATSUI, California
KATHY CASTOR, Florida
JOHN P. SARBANES, Maryland
JERRY MCNERNEY, California
PETER WELCH, Vermont
BEN RAY LUJÁN, New Mexico
PAUL TONKO, New York
YVETTE D. CLARKE, New York, *Vice Chair*
DAVID LOEBSACK, Iowa
KURT SCHRADER, Oregon
JOSEPH P. KENNEDY III, Massachusetts
TONY CÁRDENAS, California
RAUL RUIZ, California
SCOTT H. PETERS, California
DEBBIE DINGELL, Michigan
MARC A. VEASEY, Texas
ANN M. KUSTER, New Hampshire
ROBIN L. KELLY, Illinois
NANETTE DIAZ BARRAGÁN, California
A. DONALD MCEACHIN, Virginia
LISA BLUNT ROCHESTER, Delaware
DARREN SOTO, Florida
TOM O'HALLERAN, Arizona

GREG WALDEN, Oregon
Ranking Member
FRED UPTON, Michigan
JOHN SHIMKUS, Illinois
MICHAEL C. BURGESS, Texas
STEVE SCALISE, Louisiana
ROBERT E. LATTA, Ohio
CATHY MCMORRIS RODGERS, Washington
BRETT GUTHRIE, Kentucky
PETE OLSON, Texas
DAVID B. MCKINLEY, West Virginia
ADAM KINZINGER, Illinois
H. MORGAN GRIFFITH, Virginia
GUS M. BILIRAKIS, Florida
BILL JOHNSON, Ohio
BILLY LONG, Missouri
LARRY BUCSHON, Indiana
BILL FLORES, Texas
SUSAN W. BROOKS, Indiana
MARKWAYNE MULLIN, Oklahoma
RICHARD HUDSON, North Carolina
TIM WALBERG, Michigan
EARL L. "BUDDY" CARTER, Georgia
JEFF DUNCAN, South Carolina
GREG GIANFORTE, Montana

PROFESSIONAL STAFF

JEFFREY C. CARROLL, *Staff Director*
TIFFANY GUARASCIO, *Deputy Staff Director*
MIKE BLOOMQUIST, *Minority Staff Director*

SUBCOMMITTEE ON COMMUNICATIONS AND TECHNOLOGY

MIKE DOYLE, Pennsylvania
Chairman

JERRY MCNERNEY, California
YVETTE D. CLARKE, New York
DAVID LOEBSACK, Iowa
MARC A. VEASEY, Texas
A. DONALD MCEACHIN, Virginia
DARREN SOTO, Florida
TOM O'HALLERAN, Arizona
ANNA G. ESHOO, California
DIANA DEGETTE, Colorado
G. K. BUTTERFIELD, North Carolina
DORIS O. MATSUI, California, *Vice Chair*
PETER WELCH, Vermont
BEN RAY LUJÁN, New Mexico
KURT SCHRADER, Oregon
TONY CÁRDENAS, California
DEBBIE DINGELL, Michigan
FRANK PALLONE, JR., New Jersey *(ex officio)*

ROBERT E. LATTA, Ohio
Ranking Member
JOHN SHIMKUS, Illinois
STEVE SCALISE, Louisiana
PETE OLSON, Texas
ADAM KINZINGER, Illinois
GUS M. BILIRAKIS, Florida
BILL JOHNSON, Ohio
BILLY LONG, Missouri
BILL FLORES, Texas
SUSAN W. BROOKS, Indiana
TIM WALBERG, Michigan
GREG GIANFORTE, Montana
GREG WALDEN, Oregon *(ex officio)*

C O N T E N T S

	Page
Hon. Mike Doyle, a Representative in Congress from the Commonwealth of Pennsylvania, opening statement	1
Prepared statement	3
Hon. Robert E. Latta, a Representative in Congress from the State of Ohio, opening statement	4
Prepared statement	5
Hon. Frank Pallone, Jr., a Representative in Congress from the State of New Jersey, opening statement	6
Prepared statement	8
Hon. Greg Walden, a Representative in Congress from the State of Oregon, opening statement	9
Prepared statement	10
WITNESSES	
Dave Summitt, Chief Information Security Officer for the H. Lee Moffitt Cancer Center & Research Institute, and Fellow, Institute of Critical Infrastructure Technology	11
Prepared statement	14
Margot Saunders, Senior Counsel, National Consumer Law Center	20
Prepared statement	22
Patrick Halley, Senior Vice President, Advocacy and Regulatory Affairs, USTelecom–The Broadband Association	50
Prepared statement	52
Answers to submitted questions	117
Aaron Foss, Founder, Nomorobo	59
Prepared statement	61
SUBMITTED MATERIAL	
H.R. 946, the Stopping Bad Robocalls Act [1]	
Discussion Draft, H.R. _____, the Support Tools to Obliterate Pesky Robocalls Act [1]	
H.R. 1421, the Help Americans Never Get Unwanted Phone calls Act of 2019 [1]	
H.R. 2355, the Regulatory Oversight Barring Obnoxious Calls and Texts Act of 2019 [1]	
H.R. 721, the Spam Calls Task Force Act of 2019 [1]	
H.R. 2298, the Repeated Objectionable Bothering Of Consumers On Phones Act [1]	
H.R. 1575, the Robocall Enforcement Enhancement Act of 2019 [1]	
Letter of April 29, 2019, from Meredith Attwell Baker, President and Chief Executive Officer, CTIA, to Mr. Latta, submitted by Mr. Latta	97
Letter of April 29, 2019, from Matthew M. Polka, President and Chief Executive Officer, America's Communications Association, to Mr. Doyle and Mr. Latta, submitted by Mr. Latta	98
Letter of April 29, 2019, from Jonathan Bullock, Vice President, Corporate Development and Government, Hotwire Communications, et al., to Mr. Doyle and Mr. Latta, submitted by Mr. Latta	99
Letter of April 29, 2019, from ACA International, et al., to Mr. Doyle and Mr. Latta, submitted by Mr. Doyle	101

[1] Legislation discussed during the hearing has been retained in committee files and also is available at https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=109357.

Page

Letter of April 29, 2019, from Maureen Mahoney, Policy Analyst, and George P. Slover, Senior Policy Counsel, Consumer Reports, to Mr. Doyle and Mr. Latta, submitted by Mr. Doyle 103
Letter of April 29, 2019, from Marc Rotenberg, President, Electronic Privacy Information Center, et al., to Mr. Doyle and Mr. Latta, submitted by Mr. Doyle 105
Letter of April 29, 2019, from Brad Thaler, Vice President of Legislative Affairs, National Association of Federally-Insured Credit Unions, to Mr. Doyle and Mr. Latta, submitted by Mr. Doyle 107
Letter of April 29, 2019, from Mark Neeb, Chief Executive Officer, ACA International, to Mr. Doyle and Mr. Latta, submitted by Mr. Doyle 109
Report of ACA International, "The Impact of Call-blocking and Labeling Technologies on the Accounts Receivable Industry," submitted by Mr. Doyle 114
Letter of April 30, 2019, from Hon. Jefferson Van Drew, a Representative in Congress from the State of New Jersey, to the Subcommittee on Communications and Technology, submitted by Mr. Doyle 116

LEGISLATING TO STOP THE ONSLAUGHT OF ANNOYING ROBOCALLS

TUESDAY, APRIL 30, 2019

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON COMMUNICATIONS AND TECHNOLOGY,
COMMITTEE ON ENERGY AND COMMERCE,
Washington, DC.

The subcommittee met, pursuant to call, at 10:01 a.m., in the John D. Dingell Room 2123, Rayburn House Office Building, Hon. Mike Doyle (chairman of the subcommittee) presiding.

Members present: Representatives Doyle, McNerney, Clarke, Loebsack, Veasey, McEachin, Soto, O'Halleran, Eshoo, DeGette, Butterfield, Matsui, Welch, Cárdenas, Dingell, Pallone (ex officio), Latta (subcommittee ranking member), Shimkus, Olson, Kinzinger, Bilirakis, Johnson, Long, Flores, Brooks, Walberg, Gianforte, and Walden (ex officio).

Staff present: AJ Brown, Counsel; Jeffrey C. Carroll, Staff Director; Jennifer Epperson, FCC Detailee; Evan Gilbert, Deputy Press Secretary; Waverly Gordon, Deputy Chief Counsel; Tiffany Guarascio, Deputy Staff Director; Alex Hoehn-Saric, Chief Counsel, Communications and Consumer Protection; Jerry Leverich, Senior Counsel; Dan Miller, Policy Analyst; Phil Murphy, Policy Coordinator; Alivia Roberts, Press Assistant; Andrew Souvall, Director of Communications, Outreach, and Member Services; Mike Bloomquist, Minority Staff Director; Robin Colwell, Minority Chief Counsel, Communications and Technology; Jordan Davis, Minority Senior Advisor; Kristine Fargotstein, Minority Detailee, Communications and Technology; Margaret Tucker Fogarty, Minority Staff Assistant; Peter Kielty, Minority General Counsel; Tim Kurth, Minority Deputy Chief Counsel, Communications and Technology.

Mr. DOYLE. The Subcommittee on Communications and Technology will now come to order. The Chair recognizes himself for 5 minutes.

OPENING STATEMENT OF HON. MIKE DOYLE, A REPRESENTATIVE IN CONGRESS FROM THE COMMONWEALTH OF PENNSYLVANIA

Well, I want to welcome everyone to today's legislative hearing on solutions to a problem that we all have firsthand experience with: illegal robocalls. Today's hearing will examine the onslaught of illegal robocalls and seven legislative proposals to help address this harmful, predatory, and extremely annoying practice.

Among the bills we will consider today is Chairman Pallone's Stopping Bad Robocalls Act, which I support and am an original co-

sponsor of along with many members of this committee. This bill offers a comprehensive set of solutions that I believe can help seriously reduce the numbers of robocalls that consumers receive.

We will also consider Ranking Member Latta's STOP Robocalls Act which I have also agreed to cosponsor. While I have some concerns about this bill, Ranking Member Latta and I have agreed to work together to resolve these issues in order to advance this legislation. We will also be considering two bills from Congresswoman Eshoo, the HANGUP Act and the ROBO Calls and Texts Act, as well as Congressman Crist's Spam Calls Task Force Act of 2019 and Congresswoman Speier's ROBOCOP Act and Congressman Van Drew's Robocall Enforcement Enhancement Act of 2019.

I want to thank our panel of witnesses for appearing before us today to testify about this important issue and the legislation that is before this subcommittee.

Unwanted robocalls and texts are the top consumer complaint received by the Federal Communications Commission and the Federal Trade Commission. According to the FCC's report on robocalls, consumer complaints to the FCC have increased from 150,000 a year in 2016 to 230,000 in 2018. The Federal Trade Commission, which administers the Do Not Call Registry, received nearly 3.8 million complaints regarding robocalls last year alone.

As might be expected, the number of robocalls has exploded as well, topping out at nearly 48 billion, with a B, last year, a 57 percent increase in volume from the year before, according to the YouMail Robocall Index. That number is estimated to increase to 60 billion by the end of this year. And while some of these calls constituted legitimate alerts and reminders, those calls accounted for only 20 percent of the total amount of robocalls.

In the month of March alone, phones in my hometown of Pittsburgh received an estimated 37 million robocalls which was an eight percent increase in the number of calls we received the month before. The problem has gotten so bad that you can watch videos on the internet of people getting robocalls while they are in the middle of making a video complaining about robocalls. One of my favorites is of AT&T's CEO getting a robocall in the middle of an interview, showing that truly no one is immune to this nuisance.

Many phone service providers have begun making robocall blocking technologies like Mr. Foss' Nomorobo service available to their customers, and I applaud the efforts of those to offer these services to customers for free. I encourage all phone service providers to make these services available to their customers free of charge.

I believe that Congress and the FCC have an obligation to work with phone providers and their customers whether they may be institutions like the Moffitt Cancer Center, which is with us today to talk about this issue, or individual consumers, to not only help with the deployment of blocking technologies, but to work on addressing the underlying shortcomings of the law and our Nation's telecommunications infrastructure to help stem the tide of this harmful and predatory practice.

Thank you. I look forward to the testimony of the witnesses, and I yield the balance of my time to Congresswoman Eshoo.

[The prepared statement of Mr. Doyle follows:]

PREPARED STATEMENT OF HON. MIKE DOYLE

Welcome everyone to today's legislative hearing on solutions to a problem that we've all had first-hand experience with, illegal robocalls.

Today's hearing will examine the onslaught of illegal robocalls and seven legislative proposals to help address this harmful, predatory, and extremely annoying practice. Among the bills we will consider today is Chairman Pallone's Stopping Bad Robocalls Act, which I support and am an original cosponsor of, along with many members of the committee. This bill offers a comprehensive set of solutions that I believe can help seriously reduce the number of robocalls consumers receive.

We will also consider Ranking Member Latta's Stop Robocalls Act, which I have also agreed to cosponsor. While I have some concerns about the bill, Ranking Member Latta and I have agreed to work together to resolve these issues in order to advance this legislation.

We will also be considering two bills from Congresswoman Eshoo, the Hang Up Act and the ROBO Calls and Texts Act. As well as Congressman Crist's Spam Calls Task Force Act of 2019, Congresswoman Speier's ROBOCOP Act, and Congressman Van Drew's Robocall Enforcement Enhancement Act of 2019.

I'd like to thank our panel of witnesses for appearing before us today to testify about this important issue and the legislation before the subcommittee.

Unwanted robocalls and texts are the top consumer complaint received by the Federal Communications Commission and the Federal Trade Commission. According to the FCC's Report on Robocalls, consumer complaints to the FCC have increased from 150,000 a year in 2016 to 230,000 in 2018. The Federal Trade Commission, which administers the Do Not Call Registry, received nearly 3.8 million complaints regarding robocalls last year alone.

As might be expected, the number of robocalls has exploded as well, topping out at nearly 48 billion last year, a 57 percent increase in volume from the year before, according to the "you-mail" robocall index. That number is estimated to increase to 60 billion by the end of this year. And while some of these calls constituted legitimate alerts and reminders, those calls accounted for only 20 percent of the total amount of robocalls.

In the month of March alone, phones in my home town of Pittsburgh received an estimated 37 million robocalls, which was an 8 percent increase in the number of calls we received the month before.

The problem has gotten so bad that you can watch videos on the Internet of people getting robocalls while they are in the middle of making videos complaining about them. One of my favorites is of AT&T's CEO getting robocalled in the middle of an interview, showing that truly no one is immune to this nuisance.

Many phone services providers have begun making robocalling blocking technologies, like Mr. Foss' Nomorobo service, available to their customers, and I applaud the efforts of those who offer these services to customers for free. I encourage all phone service providers to make these services available to their customers free of charge.

I believe that Congress and the FCC have an obligation to work with phone providers and their customers, whether they be institutions like the Cancer Moffitt Center, which is with us today to talk about this issue, or individual consumers, to not only help with the deployment of blocking technologies, but to work on addressing the underlying shortcomings of the law and our Nation's telecommunications infrastructure, to help stem the tide of this harmful and predatory practice.

Thank you and I look forward to the testimony of our witnesses.

Ms. ESHOO. Thank you, Mr. Chairman, for yielding time to me, and thank you for considering two of my bills during today's hearing, the HANGUP Act and the ROBO Calls and Texts Act.

Millions of students, veterans, farmers, and homeowners have loans owed to or guaranteed by the Federal Government. In 2015, Congress created a loophole that allows companies collecting this debt to robocall borrowers without consent. The HANGUP Act is bipartisan, bicameral legislation that repeals this loophole, ensuring that all Americans are protected from these abusive robocalls.

Very importantly, last Wednesday, a Fourth Circuit Court of Appeals decision strengthened the need for the HANGUP Act because the Court found the 2015 loophole to be unconstitutional, so we

have an opportunity here. My other bill, the ROBO Calls and Texts Act, creates a division at the FCC to ensure that the Commission is responsive to the millions of requests that they do something and it compels them to act to adopt technological standards to combat robocalls.

So, I thank you, Mr. Chairman, for yielding the time to me and for taking up two of my bills. Yield back.

Mr. DOYLE. I thank the gentlelady. The Chair now recognizes my friend, Mr. Latta, the ranking member for the Subcommittee on Communications and Technology, for 5 minutes for his opening statement.

OPENING STATEMENT OF HON. ROBERT E. LATTA, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF OHIO

Mr. LATTA. Thank you, Mr. Chairman. And good morning and welcome to our panel of witnesses. Like many of my colleagues on this subcommittee, today's hearing addresses one of the top issues I hear about from my constituents when I am back home in Ohio. In fact, some of my constituents are getting so many unlawful robocalls they have stopped answering their phones.

After listening to these concerns, I introduced a bill with the chairman, the gentleman from Pennsylvania, that we will be discussing today, called the Support Tools to Obliterate Pesky Robocalls Act, or STOP Robocalls Act. Our bill would give us additional tools in our robocall toolbox to go after the bad actors. The STOP Robocalls Act would help terminate illegal call operations by streamlining the process for private entities to share information with the Federal Communications Commission about scams and further industry efforts to trace back the source of unwanted robocalls.

In addition to going after the root of the problem, our bill would also protect consumers by providing easier access to illegal robocall blocking technology. Our bill distinguishes between legitimate and illegitimate callers and recognizes that we need to go after the bad actors. I hope that the focus of today's hearing is also on how we need to stop illegal, unwanted robocalls.

While we all get annoyed by the overwhelming number of unlawful calls we receive, we also rely on our phone system for many valuable, proconsumer messages. Emergency personnel use voice services to provide evacuation notices and alerts during severe weather and other dangerous situations. Schools use voice and text services to notify parents of changes in the school schedule.

And although Ohio doesn't declare as many snow days as DC, parents like knowing when school is closing early or canceled. Financial services also use voice and text services to alert consumers to potentially unauthorized activity in their bank account. And the medical community uses voice and text services to follow-up with patients with important information and checkups after operations and remind patients of prescriptions refills, or even to confirm doctors' appointments.

But bad actors have also figured out how to take advantage of the phone system and technology that legitimate entities use to share important messages and instead manipulate the technology to trick and deceive consumers. These scammers deliberately falsify

their caller ID information to hoax consumers into thinking they are getting a call from their bank or the IRS or make the call appear that it is coming from someone in their neighborhood. This tactic known as "neighborhood spoofing" assumes that we are all likely to answer a phone call that appears to be local and is a key driver behind unwanted calls and texts to both wireline and wireless phones.

Furthermore, this type of fraudulent spoofing results in real financial harm. Scammers trick consumers into answering these calls and then use deceptive tactics to convince people, often vulnerable and trusting senior citizens, to hand over their personal information or to purchase fake goods and services.

We want to make sure that we are preserving consumers' access to desirable and, at times, lifesaving calls and text messages while also protecting them from bad actors who fraudulently spoof caller ID information to make illegal robocalls. At best, Americans find these robocalls pesky, and at worst, these illegal calls scam hardworking Americans out of their life savings.

Congress, the FCC, and the FTC have made tremendous progress working with industry to help reduce the number of illegal robocalls Americans receive. Industry has also been actively working to protect consumers from unwanted robocalls by developing a set of procedures to authenticate caller ID information associated with telephone calls to combat unlawful caller ID spoofing.

Last Congress, when I served as the chairman of the Digital Commerce and Consumer Protection Subcommittee, we held a hearing on the options and strategies that the Government and industry were employing to fight robocalls and caller ID spoofing and to provide consumers with the tools to protect themselves. We learned of tools available to empower consumers and discuss how consumer education was a key in keeping to prevent people from falling victim. However, as technology continues to evolve, so do the tactics that bad actors use to illegally spoof numbers and make fraudulent robocalls.

But despite our progress thus far, more work remains to be done to protect the American consumer. I am glad we are discussing several legislative proposals today that would do just that. I look forward to hearing from the witnesses and thank the chairman for working with me on the STOP Robocalls Act and for holding today's hearing.

And with that, Mr. Chairman, I yield back the balance of my time.

[The prepared statement of Mr. Latta follows:]

PREPARED STATEMENT OF HON. ROBERT E. LATTA

Good morning and welcome to our panel of witnesses. Like many of my colleagues on this subcommittee, today's hearing addresses one of the top issues I hear about from my constituents when I am back home in Ohio. In fact, some of my constituents are getting so many unlawful robocalls that they have stopped answering their phones.

After listening to these concerns, I introduced a bill with Chairman Doyle that we will be discussing today called the Support Tools to Obliterate Pesky Robocalls Act or STOP Robocalls Act. Our bill would give us additional tools in our robocall toolbox to go after bad actors. The STOP Robocalls Act would help terminate illegal call operations by streamlining the process for private entities to share information with the Federal Communications Commission about scams, and further industry

efforts to trace back the source of unwanted robocalls. In addition to going after the root of the problem, our bill would also protect consumers by providing easier access to illegal robocall blocking technology.

Our bill distinguishes between legitimate and illegitimate callers and recognizes that we need to go after the bad actors. I hope that the focus of today's hearing is also on how we need to stop illegal, unwanted robocalls. While we all get annoyed by the overwhelming number of unlawful calls we receive, we also rely on our phone system for many valuable, proconsumer messages. Emergency personnel use voice services to provide evacuation notifications and alerts during severe weather and other dangerous situations. Schools use voice and text services to notify parents of changes in the school schedule—and although Ohio doesn't declare as many snow days as DC- parents like knowing when school is closing early or canceled. Financial services also use voice and text services to alert consumers to potentially unauthorized activity in their bank account. And, the medical community uses voice and text services to follow up with patients with important information and check-ups after operations, remind patients of prescription refills, or even to confirm doctor's appointments.

But, bad actors have also figured out how to take advantage of the phone system and technology that legitimate entities use to share important messages, and instead manipulate the technology to trick and deceive consumers. These scammers deliberately falsify their caller ID information to hoax consumers into thinking that they are getting a call from their bank or IRS, or make the call appear that it is coming from someone in their neighborhood. This tactic, known as "neighborhood spoofing," assumes that we are more likely to answer a phone call that appears to be local, and is a key driver behind unwanted calls and texts to both wireline and wireless phones.

Furthermore, this type of fraudulent spoofing results in real financial harm. Scammers trick consumers into answering these calls and then use deceptive tactics to convince people—often vulnerable and trusting senior citizens—to hand over their personal information or to purchase fake goods and services.

We want to make sure that we are preserving consumers' access to desirable, and at times, life-saving calls and text messages while also protecting them from bad actors who fraudulently spoof caller ID information to make illegal robocalls. At best, Americans find these robocalls pesky, and at worst, these illegal calls scam hard-working Americans out of their life savings.

Congress, the FCC, and the FTC have made tremendous progress working with industry to help reduce the number of illegal robocalls Americans receive. Industry has also been actively working to protect consumers from unwanted robocalls by developing a set of procedures to authenticate caller ID information associated with telephone calls to combat unlawful caller ID spoofing.

Last Congress, when I served as chairman of the Digital Commerce and Consumer Protection subcommittee, we held a hearing on the options and strategies that the Government and industry were employing to fight robocalls and caller ID spoofing and provide consumers with tools to protect themselves. We learned of tools available to empower consumers and discussed how consumer education was key in helping to prevent people from falling victim.

However, as technology continues to evolve, so do the tactics that bad actors use to illegally spoof numbers and make fraudulent robocalls. Despite our progress thus far, more work remains to be done to protect American consumers. I am glad we are discussing several legislative proposals today that would do just that.

I look forward to hearing from the witnesses, and I thank the chairman for working with me on the STOP Robocalls Act and for holding today's hearing. With that I yield back.

Mr. DOYLE. I thank the gentleman. The Chair now recognizes Mr. Pallone, chairman of the full committee, for 5 minutes for his opening statement.

OPENING STATEMENT OF HON. FRANK PALLONE, JR., A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NEW JERSEY

Mr. PALLONE. Thank you, Chairman Doyle.

One of this committee's top priorities is putting consumers first, and one of the things I hear most from consumers back home is that they are sick and tired of robocalls. Consumers today are fac-

ing more robocalls than ever. Government data from 2017 shows that New Jerseyans filed more complaints with the National Do Not Call Registry per capita than any other State about robocalls.

And it is getting so bad that some experts estimate that almost half of all calls to our cell phones this year will be robocalls. And we all know how annoying these calls are, but they are more insidious than that. Robocalls are not just being made for telemarketing, some callers are trying to defraud hardworking Americans and seniors in particular. In some instances, criminals are pestering consumers with one-ring calls hoping that they will call the number back and incur excessive charges.

And Congress has taken bipartisan action in the past to help put consumers back in control of their cell phones. In 1991, Congress passed the Telephone Consumer Protection Act and then later authorized the Do Not Call Registry, but as technology has evolved robocalls and the threats they impose have simply increased. It is easier than ever for someone to begin making robocalls. Bad actors only need a smartphone with a few select applications to make spoofed robocalls. This means that existing approaches to stopping these calls may not work anymore.

And so, we need to implement new call authenticity technologies to clear these unwanted calls from our phone lines. Regulators in industry need better tools to protect consumers and once again it is time for Congress to act. Earlier this year, I introduced the Stopping Bad Robocalls Act to turn the tide in the fight against robocalls. And there is no one silver bullet and that is why it is so important that we address this problem for every side. We have a number of bills that are being considered today, as the chairman said, in this legislative hearing.

But with regard to my bill, the Stopping Bad Robocalls Act, it would require that carriers implement new call authenticity technologies to help ensure that consumers know who is on the other end of the line when they pick up the phone and implementing these technological solutions would also help consumers control who can reach them more generally.

My bill would also update the legal definition of autodialer to make sure that callers can't use new technologies to get around the longstanding consumer protections against robocalls. The FCC is currently studying how it could address its own interpretation of the term "autodialer," and as part of that proceeding the FCC could begin to fix the problem on its own. And when coming to a resolution, I would urge the Commission to put consumers first in this matter so that Congress doesn't have to redo its work.

I am hopeful the Commission will do that and, after all, they took a very proconsumer approach to revision that I included in this legislation last Congress, and that provision requires the FCC to implement a reassigned number database to ensure that when a consumer gets a new telephone number, they aren't receiving the robocalls from the person that had the number before. In December, the FCC adopted an order to implement a reassigned number database much like the one that is in my bill and I applaud this action and I look forward to the FCC getting this database operational as quickly as possible.

So, as I said, we have six bills today. There are some from Democrats, some from Republicans. One of the bills before us was introduced by the Subcommittee Ranking Member Latta. We look forward to discussing how to move bipartisan legislation forward. And we also have proposals from Representatives Van Drew, Crist, and Speier that help push the conversation forward, and we have two bills introduced by Representative Eshoo as well. So, I look forward to working in a bipartisan fashion to finally stop the onslaught of these annoying calls and appreciate the fact that we have so many Members that are trying to address this.

Thank you, Mr. Chairman. Unless anyone else wants my minute—and I don't think so. Thank you.

[The prepared statement of Mr. Pallone follows:]

PREPARED STATEMENT OF HON. FRANK PALLONE, JR.

One of this committee's top priorities is putting consumers first—and one of the things I hear most from consumers back home is that they are sick and tired of robocalls.

Consumers today are facing more robocalls than ever. Government data from 2017 shows that New Jerseyans filed more complaints with the National Do Not Call Registry per capita than any other State about robocalls. It is getting so bad that some experts estimate that almost half of all calls to our cell phones this year will be robocalls.

We all know how annoying these calls are, but they are more insidious than that. Robocalls are not just being made for telemarketing, some callers are trying to defraud hard working Americans and seniors. In some instances, criminals are pestering consumers with one-ring calls hoping that they will call the number back and incur excessive charges.

Congress has taken bipartisan action in the past to help put consumers back in control of their cell phones. In 1991, Congress passed the Telephone Consumer Protection Act and then later authorized the Do Not Call Registry. But as technology has evolved, robocalls, and the threat they impose, have increased.

It is easier than ever for someone to begin making robocalls. Bad actors only need a smartphone with a few select applications to make spoofed robocalls. This means that existing approaches to stop these calls may not work anymore. We need to implement new call authentication technologies to clear these unwanted calls from our phone lines.

Regulators and industry need better tools to protect consumers, and once again, it is time for Congress act. Earlier this year I introduced the Stopping Bad Robocalls Act to turn the tide in the fight to against robocalls. There's no one silver bullet, and that's why it is so important that we address this problem from every side.

For example, the Stopping Bad Robocalls Act would require that carriers implement new call authentication technologies to help ensure that consumers know who is on the other end of the line when they pick up the phone. Implementing these technological solutions would also help consumers control who can reach them more generally.

My bill would also update the legal definition of autodialer to make sure that callers can't use new technologies to get around the long-standing consumer protections against robocalls. The Federal Communications Commission (FCC) is currently studying how it could address its own interpretation of the term autodialer, and as part of that proceeding, the FCC could begin to fix the problem on its own. When coming to a resolution, I would urge the Commission to put consumers first in this matter so that Congress doesn't have to redo its work.

I am hopeful the Commission will do just that, after all they took a proconsumer approach to a provision I included in this legislation last Congress. That provision required the FCC to implement a reassigned number database to ensure that when a consumer gets a new telephone number, they aren't receiving the robocalls from the person that had the number before. In December the FCC adopted an order to implement a reassigned number database much like the one in my bill. I applaud this action, and I look forward to the FCC getting this database operational as quickly as possible.

Other than my bill, we will be discussing six other proposals today from both Democrats and Republicans. One of the bills before us was introduced by Sub-

committee Ranking Member Latta. I look forward to hearing about his bill and discussing how to move bipartisan legislation forward quickly.

We also have proposals from Representatives Van Drew, Crist, and Speier that help push the conversation forward. Additionally, we will discuss two bills introduced by Representative Eshoo.I look forward to working in a bipartisan fashion to finally stop the onslaught of these annoying calls.

Mr. DOYLE. The gentleman yields back. The Chair now recognizes Mr. Walden, the ranking member of the full committee, for 5 minutes for his opening statement.

OPENING STATEMENT OF HON. GREG WALDEN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF OREGON

Mr. WALDEN. Thank you, Mr. Chairman. Thanks for having this hearing. And I want to thank our panelists for being here today to help inform our work. Nothing brings us, Democrats and Republicans, together faster or stronger than I think this issue and so we look forward to working with all of you to get results.

You know, I have done 20 town halls in my district so far this year, and I can't think of a time that this question didn't come up about what are you doing to stop robocalls and these unwanted cell calls. And usually in the middle of those town halls I would get one of those as well, one of those calls. And so, I didn't answer it by the way, but I let them go to voice mail and if they don't leave a message they don't exist in my world.

So, I am all for going after these like I was for going after those people that did the pop-up ads, remember those? When you try and open a software—now we are seeing who is old here, but the pop-up ads that would occur anytime you opened up your computer. I was for the death penalty for those people, because you couldn't get anything done. And this has escalated to the same place, I think, for consumers, and they have had it and they have rightfully had it, and we have had it. And so, you are seeing an all-hands-on-deck approach here.

Now, last Congress, we passed the RAY BAUM'S Act that gave the FCC some additional authority in this space as well and that was a big bipartisan bill we joined together. I know, Mr. Chairman, we are going to have the FCC fully before the committee. This would be a good topic to raise with them as well because I know Chairman Pai and others are clearly involved in this.

But we all benefit by the hearing today. It was a year ago almost to the day that we held a hearing on this very topic, and I think maybe, Mr. Foss, you were here for that. And we appreciated your testimony at that time and we shared several ideas on how industry could do more in this area to stop this scourge, and our consumers should take and make use of the solutions that our really bright innovators are putting forward. We will soon, as I say, have the FCC before us.

I am pleased we have these bills, a wide range assortment of different legislative initiatives here to go after this issue, so I am pleased that we've got a lot of options before us. As we work to make this a bipartisan success, I know it can be under the chairman's leadership, I do not want to build a false expectation that these bills will end the problem, because that is part of what we

learned out of the testimony from the hearing a year ago, is just how difficult this is because of its international component.

Subcommittee members here know better than many on how communications and technologies are constantly evolving. The bad actors' tricks evolved beyond our Do Not Call Registry and will likely figure out an avenue beyond our next effort, so we have got to stay vigilant. However, the more friction we create against these criminals, and I call them criminals because they are, and the more focused, public-private partnerships amongst industry, consumer groups, and government are in rooting out the problems, I think we can make some real strides here and gain in helping American consumers.

Lastly, while engagement of law enforcement is beyond the purview of our committee, that is an avenue worth pursuing as well as I look forward to the bills being considered today being further strengthened by a dialogue with our friends in the Senate who have also sought to engage the powers of the Attorney General.

So again, I want to thank our witnesses. I want to thank the chairman of the subcommittee and the full committee for having this hearing today. And if there are Members on our side that would like to use my last minute and a half or so, I would be happy to yield. And if not, Mr. Chairman, we can get on with the hearing. So, I yield back, and thank you again.

[The prepared statement of Mr. Walden follows:]

PREPARED STATEMENT OF HON. GREG WALDEN

Let me welcome the witnesses to the panel today. All of you here care deeply about the proposals before us, and all are working very hard to address this scourge—that has grown from an annoyance to a sincere peril—in your respective areas.

In the 20 townhalls I've held across my district, it seemed like inevitably someone would ask "can't something be done about robocalls?" I share their frustration and remain committed to working with the chairman to address these calls with action from Congress.

You would be hard pressed to find a technology that's more personal than a telephone. Whether it's the cell phone in your pocket, or for some, a landline at home, voice communications on these devices is still an important way in which we connect to one another. Yet that personal connection is being violated by bad actors using technology to hide their tracks. They should be treated and prosecuted for what they are, criminals. These criminal parties have done significant harm to Americans both personally and professionally.

First, as we seek a successful effort on this legislation, I believe it is important to state that we make a clear distinction in targeting those parties that have malicious intent as opposed to those who do not. Our clearest and quickest path for enacting law is to go after those that have malicious intent. To go beyond that, we will undermine services that many Americans depend upon every day.

Second, I want to put an emphasis on thanking the chairman for the process we are vetting these bills under today. By putting our teams together, it is a welcome return to the process we operated under with our friends last Congress that led to many bipartisan successes, one of which specifically sought to address malicious spoofing. As part of RAY BAUM's Act last Congress we provided the FCC more authority to go after bad actors who utilize calls and texts. A bipartisan process matters. We all benefit from hearing and debating each other's ideas. Such vetting gives us the opportunity to get to the heart of the problem, and not error on the side of cutting off legitimate use of these technologies, such as protecting the anonymity of a shelter assisting at-risk individuals, alerting you to a fraudulent use of your credit card, or providing you the simple convenience of interacting with your ride-share service.

Almost a year ago to the day, we held a hearing on combating illegal and fraudulent robocalls and spoofing. We shared several ideas on how industry can do its part

to address this scourge, and how consumers should make use of the solutions. We will soon have the FCC before the committee, and we will gain by their technical insight before we mark-up. I'm pleased that the bills we review today seek to lock in those objectives. As we highlighted then, we owe it to our constituents to present all options available to them.

As we work to make this a bipartisan success, and I know it can be under the chairman's leadership, I do not want to build a false expectation that these bills will end the problem. Subcommittee members here know better than many how communications and technologies are constantly evolving. The bad actors' tricks evolved beyond our Do Not Call registry and will likely figure out an avenue beyond our next effort. However, the more friction we create against these criminals, and the more focused public-private partnerships amongst industry, consumer groups, and government are in rooting out the problems, we can make great strides in regaining American's confidence in their communications.

Lastly, while engagement of law enforcement is beyond the purview of this committee, that is an avenue worth pursuing as well and I look forward to the bills being considered today being further strengthened by a dialogue with our friends in the Senate who have also sought to engage the powers of the Attorney General.

Thank you again for my colleagues and the witness panel, and I look forward to another bipartisan bicameral success originating from this committee.

Mr. DOYLE. The gentleman yields back. The Chair would like to remind Members that, pursuant to committee rules, all Members' written opening statements shall be made part of the record.

So, I would now like to introduce our witnesses for today's hearing. Mr. Dave Summitt, chief information security officer for the H. Lee Moffitt Cancer Center & Research Institute and Fellow for the Institute for Critical Infrastructure Technology, welcome.

Ms. Margot Saunders, senior counsel, National Consumer Law Center, welcome.

Mr. Patrick Halley, senior vice president, Advocacy and Regulatory Affairs, USTelecom and The Broadband Association, welcome, sir.

And, Mr. Aaron Foss, founder of Nomorobo, thank you for being here today. We look forward to your testimony.

At this time, the Chair will now recognize each witness for 5 minutes to provide their opening statement, but before we begin, I would like to explain the lighting system. In front of you is a series of lights. The light will initially be green at the start of your opening statement. The light will turn yellow when you have 1 minute remaining, and please wrap up your testimony. At that point the light will turn red when your time expires.

And with that, Mr. Summitt, you are now recognized for 5 minutes, and make sure your microphone is turned on, sir.

STATEMENTS OF DAVE SUMMITT, CHIEF INFORMATION SECURITY OFFICER, H. LEE MOFFITT CANCER CENTER & RESEARCH INSTITUTE, AND FELLOW, INSTITUTE OF CRITICAL INFRASTRUCTURE TECHNOLOGY; MARGOT SAUNDERS, SENIOR COUNSEL, NATIONAL CONSUMER LAW CENTER; PATRICK HALLEY, SENIOR VICE PRESIDENT, ADVOCACY AND REGULATORY AFFAIRS, USTELECOM–THE BROADBAND ASSOCIATION; AND AARON FOSS, FOUNDER, NOMOROBO

STATEMENT OF DAVE SUMMITT

Mr. SUMMITT. Thank you, Chairman Doyle and members of the committee. It is truly a privilege to be here and been invited to give such hopefully compelling information for you to act upon the problem we are seeing today. My name is Dave Summitt. I am the chief

information security officer for Moffitt Cancer Center in Tampa, Florida.

Moffitt is a highly recognized and, in my opinion, one of the most elite hospital, cancer hospital and care in the world. They treat 60,000 individuals on an annual basis at Moffitt, which makes them the third busiest hospital in the Nation. In addition, they are a National Cancer Institute Comprehensive Care Center, one of three—of 49, and it is truly an honor to be part of that organization.

So why I am here today is to bring more of a consumer business portion to this problem because it is a significant problem. And when I first started hearing about and getting excited, really, about what is being proposed here for stopping robocalls, one of the first things that popped into my mind was I am not sure that the general population and the powers that be that can have some say into this is understanding the real severity level of this and that is why I want to try to bring this home.

As large as we are and as much as we go through, and myself being head of the cyber operations at Moffitt trying to protect our patients and our organization and our applications, to give kind of an idea of the extent of this problem we process approximately 3 million malicious events every month at Moffitt on our network. When the telecom starts being part of this, it is just inundating as even more and it is a very bad problem. These aren't just robocalls for annoyance. And as much as all of the bills so far as addressing this problem of annoyance, this goes much deeper. It is now starting to impact patient care at facilities and healthcare across the Nation.

In my efforts of trying to raise awareness of what you are doing with our healthcare community, I used our Critical Infrastructure Information Sharing and Analysis Centers, which was stood up by the Government for purposes of reaching our critical infrastructure. Healthcare is one of the 16 critical infrastructure sectors, and because of that I got a lot of information back from various healthcare organizations across the Nation saying we have a problem and behind what I am bringing to you today is that 18 additional healthcare organizations have backed what we are trying to do and support you with doing. And inside my written testimony, you will see all 18 of these.

For an example of our problem, before I came last week, I had our telecommunications people pull our logs. We ended up with 6,600 calls in a 90-day period that were of either malicious intent or identified themselves as someone they are not. And the point I want to make about these 6,600 calls, these were calls that were called to us from the outside of our organization using our ID, our caller ID, to get into the organization.

So, when you are sitting here and you are in a healthcare situation and you are seeing a phone call come in from someone inside our organization, you are going to pick that thing up. And that is the intent of what they are trying to do in reaching us. If they get legitimacy behind the caller ID, chances are they are going to pick up the phone. Sixty-six hundred of them in a 90-day period. That equated—I also pulled the logs of how long it took for those calls

to last, 65 hours of time was taken just for those 6,600 calls. That is just one area of these calls that have been coming in.

The other calls that we are having now and we have seen a ramp-up going on is that not only are they calling our organization with it, but they are calling our community. They are calling other people outside of our organization using our ID, using our name, and not only that but they are calling these people in our communities and patients. When they pick up the phone and they see it is from Moffitt Cancer Center they are being identified on the other end as Moffitt Cancer Center employees.

So, if you can imagine, if they happen to get a hold of one of our patients and it is called Moffitt Cancer Center, they are absolutely going to answer that phone. And they are extracting information that can be detrimental to those patients.

[The prepared statement of Mr. Summitt follows:]

Testimony of Dave Summitt
H. Lee Moffitt Cancer Center & Research Institute

Before the Subcommittee on Communications and Technology
of the Committee on Energy and Commerce

"Legislating to Stop the Onslaught of Annoying Robocalls"

April 30, 2019

Good morning Chairman Doyle and members of the committee. Thank you for your invitation and providing me with the opportunity to provide information and insight to the committee on this increasingly problematic topic. It is an honor to appear before you.

My name is Dave Summitt. I am a fellow of the Institute of Critical Infrastructure Technology and I am employed as the Chief Information Security Officer over-seeing the cyber security operations for the H. Lee Moffitt Cancer Center and Research Institute located in Tampa, Florida. Moffitt provides oncology care to more than 60,000 individual patients each year, making it the third busiest stand-alone cancer hospital in the United States. Moffitt is also one of forty-nine National Cancer Institute's Designated Comprehensive Cancer Centers. This distinction is earned by demonstrating excellence in conducting scientific research and translating it into more effective cancer treatments and prevention methods. The organization is driven by excellence and it is my privilege to be part of this outstanding institution.

I am here today not only on behalf of Moffitt but also for numerous other health-related organizations that have signed on with us to endorse your efforts in addressing the serious issue before you. My ultimate goal for today's testimony is to give a voice to the hundreds of organizations that are experiencing the impact of unsolicited, fraudulent, and malicious telephone calls. When received, these calls are disruptive and potentially dangerous. Moreover, parties initiating these calls are deceptively identifying our organizations as the source, which is damaging to our reputation and, more importantly, the welfare of our communities

Every day, we are overwhelmed with new security threats and the health care sector, a United States critical infrastructure, continues to be a prime target. The health and livelihood of millions of Americans are at stake when the security of medical and financial records is compromised and healthcare operations are interrupted or shut-down.

For this reason, we greatly appreciate the efforts driven by members of the U. S. House of Representatives to address the threats posed by the malicious use of robocalls and other telephone-calling methods to gain access to, and fraudulently use sensitive data from consumers and businesses.

In our experience, this activity constitutes a serious threat to patient care, in addition to disrupting business operations and facilitating financial fraud. In recent months, many consumers, including some patients and their families, have been targeted by robocallers who use "spoofed" numbers identical to the hospitals in an effort to gain sensitive information. Even more concerning is that this practice can jeopardize the line of communication between health providers and patients by casting doubt on the integrity of calls coming from the hospital or their care provider.

What I bring to the committee is information that elevates this issue beyond the level of just an "annoyance"; these are outright fraudulent calls with malicious intent. The core problem is that calls are permitted to originate with deceptive information making the Caller ID product ineffective. The term "robocall" is generally associated with marketing firms attempting to solicit you for their product by automatically stepping through a database of phone numbers. Robocalling is only the tip of the proverbial iceberg.

Respectfully, I am not minimizing the frustration this causes for the individual consumer. In fact, on my personal cell phone I have forty-five blocked numbers entered just in the last ninety days. However, as the Chief Information Security Officer of a large organization, it rises to a much higher level than just an annoyance. They use a common cyber-attack technique called "social engineering." This relies heavily

on human interaction to trick people into letting their guard down and breaking standard security practices. When successful, social engineering attacks enable attackers to gain legitimate, authorized access to confidential information. These SPAM calls are the equivalent to SPAM emails, where the sender hides behind a façade that seems legitimate, but in reality can be an attempt to cause harm or obtain financial gain.

I am presenting to the committee three situations that represent the greatest concern for our organization. First, we receive calls that are made to look like they are coming from within our organization. Our employees see our own number on their caller ID and give no thought to answering, only to be speaking with someone with malicious intent. Second, there are calls going out to individuals across the nation where the caller ID indicates it is coming from Moffitt Cancer Center. When the recipient answers, they are greeted with someone identified as Moffitt personnel who then proceeds to ask for insurance or other payment information. The third types of call we receive are targeting specific individuals to obtain confidential information, a form of spear phishing. These calls are identified as a reputable source, such as law enforcement or a government entity, which is what heightens the likelihood of success.

To amplify the extent of this problem, I am sharing data from our organizational phone system for the past ninety days. During this time period we received over 6,600 external calls identified as a Moffitt internal phone number consuming a total of 65 hours of response time. Also concerning is that in one recent 30 day period, over 300 calls were made to Moffitt Cancer Center coming from the Washington DC area. Over half of these calls were from numbers that represented some form of federal agency identity; some were legitimate but most were not. In one recent example, the fraudulent calls that impacted Moffitt were identified as coming from the U.S. Department of Justice using a legitimate phone number. When our employees answered the phone, they were subjected to an urgent request by

the caller who self-identified as a DOJ employee. They demanded to speak with the named physician - and only that physician - and communicated an urgent problem affecting his medical license number and his Drug Enforcement Agency number. These attempts occurred over several weeks and involved numerous care providers. These calls can be quite disturbing and disruptive, and we, along with other organizations have to manage them on a daily basis.

By enacting strong consumer protections and empowering the FCC with strong enforcement tools to rein in this damaging activity, we believe that HR946, the Stopping Bad Robocalls Act could help curb these abusive practices. We also commend HR 721, the Spam Calls Task Force Act, which would establish an interagency working group to devise ways to address this threat through enforcement and regulation. I am encouraged to know that the committee is also considering other worthwhile legislation submissions.

As this Committee considers new legislative and regulatory strategies to address these issues, I would ask that three things be considered: First, place provisions for accurate caller identification into your requirements; Second, place some of this burden and responsibility back onto the telecom carriers and third; provide requirements for telecoms to work with businesses in shutting down or investigating malicious activity, especially when it involves a critical infrastructure.

My request for strengthening accountability and cooperation by telecommunications carriers is based on recent interactions in our fight against malicious activity. During two recent incidents, we contacted our carrier for assistance and received inadequate support. During the aforementioned U.S. Dept of Justice event, the telecommunications carrier told us that we needed twenty to twenty-five calls within a 72 hour window before we could file a complaint with them. The carrier's internal investigations group had defined this threshold independently on the impact it had on our operations. During a second incident, when we were investigating numerous malicious calls identified with our own organization's

number, the carrier would not give us the source of the calls and stated a subpoena would be necessary to obtain the information. I am rather astonished that others can use our owned phone number range, fraudulently represent our organization, and we have no recourse other than court order. There should be provisions made that when a company is actively investigating a suspected fraud or information security breach, they should have cooperation from the carrier. Our health care regulations require us to protect patient privacy and safety, yet it seems bad actors are more easily protected from privacy than those already covered under regulatory requirements. We are living in a high-tech age and capabilities already exist to remedy this situation, but they are not being employed. When a person receives a call identified as the "U.S. Dept of Justice", is it unreasonable to expect that it is originating from a legitimate source and not a malicious actor falsely using this identify? Borrowing a phrase from Chairman Doyle's opening statement in last month's markup meeting of H.R. 1644, you have an opportunity to "put in place 21st Century rules for a 21st Century" technology.

Moffitt and the following organizations offer our support for your efforts to curb telecommunication malicious activity. Furthermore, we hope you will count us as a resource to assist you in protecting the critical health care infrastructure. These organizations cover nine states and the DC area:

From Ranking Member Rep. Latta's state of Ohio: Genesis Health System

From committee member Rep. Soto's state of Florida:
Tampa General Hospital, Baycare Health System, Orlando Health, Apex Digital Imaging and Security Compliance Associates

From committee member Rep. Clarke's state of New York
Wellspan Health, Memorial Sloan Kettering Cancer Center and Nicholas H. Noyes Memorial Hospital

From committee member Rep. Butterfield's state of North Carolina: New Hanover Regional Medical Center

Yale New Haven Health System – Connecticut

Premise Health – Tennessee

Faith Regional Health Services - Nebraska

College of Healthcare Information Management Executives – Michigan

Institute for Critical Infrastructure Technology – Washington DC

SAP National Security Services - Pennsylvania

Thank you for your time and attention.

Mr. DOYLE. Well, thank you, Mr. Summitt.

Ms. Saunders, you are recognized for 5 minutes.

STATEMENT OF MARGOT SAUNDERS

Ms. SAUNDERS. Thank you, Chairman Doyle, Mr. Latta, and members of the committee. I appreciate the opportunity to testify today on behalf of the low-income consumers of the National Consumer Law Center and three other national groups.

We are here today specifically in strong support of H.R. 946. Last month, as you know, Americans received 5.2 billion robocalls, the majority of which are not overt scams but they are unwanted calls made at the behest of American businesses engaged in telemarketing and collecting debts. Passage of 946 will stop these unwanted robocalls. American businesses are responsible for most of the intrusive telemarketing calls selling car insurance, health insurance, car warranties, home security systems, resort vacations and the like.

And more and different American corporations make billions of robocalls to collect debts. Credit card companies admit to making three to five calls per account per day. Debt collectors admit to making a billion debt collection calls every year. The Telephone Consumer Protection Act was supposed to protect us from unwanted robocalls simply by requiring that all automated calls can only be made to cell phones with consent or prerecorded calls engaged in telemarketing must have written consent when they are made to land lines.

But the recent escalation in robocalls is likely due to the anticipated caller-friendly response by the FCC, by the Federal Communications Commission, to loosen restriction on robocalls, which is evidenced by the chart that I have on page 8 of my testimony, that followed the recent decision by the DC Circuit Court in *ACA* v. *FCC* that, among other things, sent back to the FCC what the technical definition of an automated dialer is.

The calling industry's response to this decision illustrated by the request of the U.S. Chamber of Commerce, joined by 16 national industries, requested the FCC to loosen restrictions on robocalls. The Chamber and the other callers are pushing the FCC and the courts to interpret the definition of autodialer in such a way that it will not cover any systems currently in use. This is not supported by either the statute, the logic, or the legislative history. If their requests are granted, the number of automated calls will skyrocket and there will be no protections whatsoever against automated texts.

And we may not be even able to tell callers to stop calling once we have given them our consent initially. The FCC has the authority to interpret these issues correctly, but Congress can protect consumers unequivocally by passing H.R. 946. For example, one clarification that 946 would make is defining autodialer to include the automated text messaging system that last year was found by the Third Circuit that sent 27,000 unwanted text messages to one consumer to not be a covered autodialer. Or the 56 million automated calls by Hilton Grand Vacations that were to sell vacations to consumers where the Hilton claims these were not covered by the TCPA so that consent is not required.

Other sections of 946 are also essential. We really support the authentication requirements, the wrong number rules, the limiting of exemptions and strengthening enforcement. But here is the dynamic. Passage of H.R. 946 will clearly and unequivocally address the problem of unwanted robocalls. The robocallers, the telemarketers, the debt collectors, and others will object strenuously. It is up to Congress to protect us and to protect the integrity of the American telephone system from the scourge of unwanted robocalls. I would be happy to answer any questions. Thank you.

[The prepared statement of Ms. Saunders follows:]

Testimony before the

HOUSE COMMITTEE ON ENERGY AND COMMERCE

Subcommittee On Communications and Technology

Regarding

"Legislating to Stop the Onslaught of Annoying Robocalls"

Testimony written and presented by:

Margot Freeman Saunders
Senior Counsel
National Consumer Law Center

On behalf of
the low-income clients of the
National Consumer Law Center

and

Consumer Federation of America
Consumer Action
National Association of Consumer Advocates

April 30, 2019

Margot Saunders
National Consumer Law Center
1001 Connecticut Ave, NW
Washington, D.C. 20036
(202) 452 6252
msaunders@nclc.org
www.nclc.org

Legislating to Stop the Onslaught of Annoying Robocalls
April 30, 2019

Chairman Doyle, Chairman Pallone, Congressman Latta, and Members of the Committee, I appreciate the opportunity to testify to strongly support H.R. 946: the Stopping Bad Robocalls Act. I provide my testimony here today on behalf of the low-income clients of the **National Consumer Law Center (NCLC)**,[1] and on behalf of **Consumer Action, Consumer Federation of America,** and the **National Association of Consumer Advocates.**

I. Introduction

Americans were subjected to *5.2 billion* robocalls last month--an increase by a remarkable 370% just since December 2015.[2] This explosion of robocalls invades our privacy, distracts us, disrupts our lives, costs us money, and undermines the utility of the American telephony system.

These problem robocalls are not just overt scams, such as calls made by criminals to steal identities or defraud people into making payments to avoid spurious threats. As I explain in section II below, and illustrate in the attached Appendix, major American corporations, many of which are household names, significantly contribute to the proliferation of robocalls plaguing Americans every day. These corporations are the defendants in actions in the federal courts in almost every state, and, more tellingly, they are generally the leaders in the effort currently waging in the halls of the Federal Communications Commission (FCC) to weaken critical interpretations of the Telephone Consumer Protection Act (TCPA).[3] These callers are claiming to be the victims of a TCPA crisis—but it is a crisis of their own creation. The primary goals of this testimony are to illustrate this, and show why passage of H.R. 946 is necessary to protect consumers.

The premise of the TCPA is straightforward. It does not prohibit all robocalls. The TCPA and the regulations that implement the TCPA have two simple requirements with respect to robocalls and robotexts. First, a call or text can be made to a cell phone using an automatic telephone dialing system (ATDS) or a prerecorded voice only with the prior express consent of the person called, and the consent must be in writing if it is a telemarketing call. Second, prior express written consent is also required for any prerecorded telemarketing call to a residential line. (There are exceptions for

---

[1] This testimony was written with the substantial assistance of NCLC Deputy Director Carolyn Carter and researcher Emily Green Caplan.

[2] *See* YouMail Robocall Index, *available at* https://robocallindex.com/ (last accessed Apr. 4, 2019).

[3] 47 U.S.C. § 227.

calls relating to an emergency or to collection of a debt owed to the United States.[4]) The elegance of this construct is that it gives us—the people being called-- control over our own phones.

The problem is that the callers want to make the robocalls without worrying about having that consent. And they do not want to stop calling when consumers say "stop."

The Federal Communications Commission (FCC) currently has pending before it several proceedings in which critical interpretations of the TCPA will be provided, many of which were necessitated by the D.C. Circuit's decision last year in *ACA International v. F.C.C.*[5] This decision sent back to the FCC important issues about how to define covered automated telephone dialing systems, how to deal with wrong number calls, and how to deal with revocation of consent. The FCC requested comments on these issues and related ones in the spring of 2018.[6]

The FCC already has the authority to make all the right decisions under the current version of the TCPA. However, the same callers that are responsible for so many of the robocalls plaguing our cellphones are also pushing both the FCC and the courts to create loopholes and allow evasions of the rules in the TCPA so that these callers can make more robocalls, unrestrained by the consent requirements of the law. Section 2 of H.R. 946 will protect consumers from unwanted robocalls by ensuring that the FCC will not make the wrong decisions on these interpretative questions. The other sections of H.R. 946 are also critically important to protect consumers from unwanted robocalls regardless of the FCC's interpretations of the TCPA.

In this testimony, I will first address the fact that it is major American corporations that are responsible for most of the robocalls we all deplore, and discuss why the number of calls is escalating so alarmingly. I will then discuss the need for each of the provisions of H.R. 946.

II. Major American Corporations Are Responsible for the Majority of Robocalls.

The majority of robocalls are made by, or at the behest of, major American corporations—

---

[4] Just last week, however, the exception allowing calls to collect debt owed the federal government was ruled unconstitutional by the Fourth Circuit. Am. Ass'n of Political Consultants, Inc. v. Fed. Commc'ns Comm'n, ___ F. 3d ___, 2019 WL 1780961 (4th Cir. Apr. 24, 2019) (exemption is content-based restriction on speech in violation of Free Speech Clause and is severable from remainder of TCPA).

[5] 885 F.3d 687 (D.C. Cir. 2018)

[6] *See, e.g.,* Public Notice, Federal Communications Commission, Consumer and Governmental Affairs Bureau Seeks Comments on Interpretation of the Telephone Consumer Protection Act in Light of the D.C. Circuit's ACA International Decision, CG Docket Nos. 18-152 and 02-278 (Rel. May 14, 2018), *available at* https://ecfsapi.fcc.gov/file/0514497027768/DA-18-493A1.pdf.

large, respected national corporations with whom many of us do business every day are responsible for hundreds of millions of unwanted robocalls every month. The majority of robocalls made every day to our home phones and our cell phones are not overt scam calls, but calls made by so-called "legitimate businesses."[7]

Telemarketing. Major American corporations make directly—or are responsible for—a vast number of intrusive, annoying, repeated telemarketing calls to our landlines and cell phones--selling car insurance,[8] health insurance,[9] car warranties,[10] home security systems,[11] resort vacations,[12] and more. Some of these calls push products and services that are shoddy, overpriced, or of dubious value, and some may push real bargains, but all of these calls annoy us, interrupt us, and invade our privacy. If the rate of telemarketing calls continues at the current pace, in 2019 there will be almost 10 billion telemarketing robocalls made in the United States.[13]

---

[7] In 2018, the average monthly breakdown of robocalls by category, as reported by YouMail's Robocall Index, was: 37% scams, 23% debt collection calls (including payment reminders), 18% telemarketing, and 22% alerts and reminders. In March of 2019, that same breakdown was 47% scams, 20% alerts and reminders, 17% debt collection calls (including payment reminders), and 16% telemarketing. www.Robocallindex.com.

The YouMail Robocall Index estimates the monthly robocall volume in the U.S. by extrapolating data collected from calls made to its users. In a letter from YouMail's CEO Alex Quilici to NCLC Senior Counsel Margot Saunders, Mr. Quilici noted that YouMail's analysis generally classifies calls dialed for debt collection, telemarketing, and other legitimate business purposes as scam calls if the caller "spoofs" the call to mask its true origins, so the 47% figure includes both calls by outright fraudsters and these spoofed calls from legitimate American businesses.

[8] *See* Smith v. State Farm Mut. Auto. Ins. Co., 30 F. Supp. 3d 765 (N.D. Ill. 2014).

[9] *See* Sullivan v. All Web Leads, Inc., 2017 WL 2378079 (N.D. Ill. June 1, 2017). *See also* Northrup v. Innovative Health Ins. Partners, L.L.C., 329 F.R.D. 443 (M.D. Fla. 2019) (text messages).

[10] *See* Mey v. Enterprise Fin. Group, Case No. 2:15-cv-00463 (M.D. Fla. filed Aug. 3, 2015).

[11] *See In re* Monitronics Int'l Inc., Telephone Consumer Prot. Act. Litig., Case No. 1:13-md-02493 (N.D. W. Va. filed Feb. 28, 2014). *See also* Braver v. NorthStar Alarm Servs., L.L.C., 329 F.R.D. 320 (W.D. Okla. 2018) (regarding 75 million prerecorded voice calls to sell home security systems).

[12] *See* Glasser v. Hilton Grand Vacations Co., L.L.C., 341 F. Supp. 3d 1305 (M.D. Fla. 2018), *appeal to 11th Circuit pending.*

[13] Taking the average monthly robocall totals for the first three months of 2019, as reported by YouMail in its Robocall Index (www.Robocallindex.com), U.S. consumers will receive an estimated 61.2 billion robocalls in 2019. Over the same three-month period, YouMail estimates that 15.7% of robocalls were telemarketing calls. If telemarketing calls continue at the current pace, U.S. consumers will receive nearly 10 billion telemarketing robocalls in 2019. (The monthly average for all robocalls in the first three months of 2019 is 5.1 billion; the average telemarketing percentage is 15.7%. The estimate for the total for all robocalls in 2019 is 61.2 billion; 15.7% of that total is 9.6 billion.) And these numbers do not reflect the calls that YouMail has not included in the telemarketing numbers because the caller IDs were spoofed, which calls were therefore included in the count for scam calls.

There are dozens of cases against corporate defendants seeking redress for tens of millions of unwanted and illegal telemarketing robocalls. Just a few of these cases holding American corporations responsible for making hundreds of millions of telemarketing calls include—

- **Insurance:** *Smith v. State Farm Mut. Auto. Ins. Co.*[14] In this case, the court held State Farm liable for the TCPA violations of a lead-generator marketing company it had used to market its insurance products. Calls were made to over 80,000 consumers.
- **Home Security Systems:** *Mey v. Monitronics Int'l, Inc.*[15] The named plaintiff had received over 19 calls from a broker calling to sell home security services, even though she had listed her telephone number on the national Do Not Call Registry. These telemarketing calls were made by lead generators on behalf of a Monitronics dealer. Calls were made to more than 7.7 million phone numbers. Monitronics claimed that it was not responsible for these calls made by others to sell its services.
- **Cruises:** *McCurley v. Royal Seas Cruises, Inc.*[16] This case challenged the legality of 634 million calls[17] to the cell phones of 2.1 consumers[18] in violation of the TCPA. The court allowed the case to proceed as a class action despite the cruise line's claim that it was not responsible for the calls made by lead generators, who referred interested consumers to Royal Seas after telemarketing calls.
- **Mortgage Lending**: *Ott v. Mortgage Investors Corp. of Ohio, Inc.*[19] A mortgage lender robocalled over 3.5 million people to push them into refinancing their mortgages with loans guaranteed by the U.S. Department of Veterans Affairs.
- **Vacations:** *Glasser v. Hilton Grand Vacations Co., L.L.C.*[20] This case challenges whether 56 million calls made to sell Hilton vacations were covered by the TCPA, as the telemarketer claimed the robocalls were not made with a covered autodialer.
- **Satellite Television:** *Krakauer v. Dish Network, L.L.C.*[21] This case challenged the millions of robocalls made by Dish's independent contractors, for which Dish disclaimed liability. The trial court held Dish liable.
- **Film Studio:** *Golan v. Veritas Entertainment, L.L.C.*[22] A film studio made over three million unsolicited calls as part of a six-day telemarketing campaign to promote the film "Last Ounce of Courage."
- **Business Services Provider:** *Thomas v. Dun & Bradstreet Credibility Corp.*[23] This provider made repeated telemarketing calls, even after requests to stop, to advertise business

---

[14] 30 F. Supp. 3d 765 (N.D. Ill. 2014).

[15] 959 F. Supp. 2d 927 (N.D. W. Va. 2013). *See also In re* Monitronics Int'l, Inc., Telephone Consumer Prot. Act. Litig., Case No. 1:13-md-02493 (N.D. W. Va. filed Aug. 31, 2017) (settlement agreement)

[16] 2019 WL 1383804 (S.D. Cal. Mar. 27, 2019).

[17] *Id.* at *9.

[18] *Id.* at *10.

[19] 65 F. Supp. 3d 1046 (D. Or. 2014).

[20] 341 F. Supp. 3d 1305 (M.D. Fla. 2018), *appeal to 11th Circuit pending.*

[21] 311 F.R.D. 384 (N.D.N.C. 2015)

[22] 2017 WL 2861671 (E.D. Mo. July 5, 2017).

services to over one million individuals.

There are dozens of similar cases filed in courts around the nation every month. Appendix 1 is a list of just 33 samples of the cases addressed by the courts in the past two years, provided to illustrate the pervasiveness of these telemarketing calls from American businesses, as well as the variety of excuses that these businesses typically provide for why their automated calls to American households should not be covered by the TCPA. And a review of the enforcement actions filed by the Federal Trade Commission (FTC) shows that, in the past 10 years, it filed 151 cases for illegal telemarketing, almost all of which were against American businesses.[24] Indeed, some of the defendants in the actions brought by the FTC then turned around and asked the FCC for exemptions or retroactive waivers of liability for their TCPA violations.[25] Similarly, many of the actions brought by the FCC against illegal robocallers are against American businesses.[26]

Debt Collection Calls. In addition to telemarketers, major American corporations make an enormous number of robocalls to collect debts. The creditors with whom we all do business regularly make millions of unwanted robocalls daily to collect debts,[27] and debt collectors admit to making at least a billion debt collection calls per year.[28]

Many of these robocallers repeatedly and flagrantly violate the consumer protections of the TCPA, simply paying off consumers when they are sued, and then continuing their pattern of calling.

---

[23] Case No. 2:15-cv-03194 (C.D. Cal. filed Apr. 28, 2015).

[24] The results of an advanced search on the FTC's website are available at: https://www.ftc.gov/enforcement/cases-proceedings/advanced-search?combine=&field_case_action_type_value=All&field_federal_court_tid=All&field_matter_number_value=&field_industry_tid=All&field_enforcement_type_tid=All&field_mission_tid_1=2973&field_competition_topics_tid=All&field_consumer_protection_topics_tid=236&field_release_date_value%5Bmin%5D%5Bdate%5D=&field_release_date_value%5Bmax%5D%5Bdate%5D=&date_filter%5Bmin%5D%5Bdate%5D=&date_filter%5Bmax%5D%5Bdate%5D=&items_per_page=100.

[25] *See, e.g.,* NorthStar Alarm Services, Petition for Expedited Ruling Clarifying 47 U.S.C. § 227(b)(1)(B) of the Telephone Consumer Protection Act (filed Jan. 2, 2019), *available at* https://ecfsapi.fcc.gov/file/10103290733918/NorthStar%20FCC%20Petition.pdf.

[26] See Federal Commc'ns Comm'n, Telephone Consumers Division – Robocall, *available at* https://transition.fcc.gov/eb/tcd/Robocall.html.

[27] Credit card companies admit that their collectors make 3 to 15 calls *per account* per day. *See* Consumer Fin. Prot. Bureau, The Consumer Credit Card Market 313 (Dec. 2017), *available at*

https://files.consumerfinance.gov/f/documents/cfpb_consumer-credit-card-market-report_2017.pdf.

[28] ACA International White Paper, Methodological and Analytical Limitations of the CFPB Consumer Complaint Database 7 (May 2016), *available at* https://www.acainternational.org/assets/research-statistics/aca-wp-methodological.pdf ("It is estimated that the debt collection industry makes over one billion consumer contacts on an annual basis . . . .").

But debt collection robocalls remain a top complaint by consumers. Many debt collection calls are made to people who owe money and are behind on their payments, but many others are made to people who have nothing to do with the debts.

Below are just a few examples of problematic debt collector robocallers. These cases all involve hundreds—if not thousands—of calls, and all involve multiple calls after repeated requests from the consumer to stop calling.

1. *Robertson v. Navient Solutions.*[29] Shortly after Ms. Robertson acquired a Certified Nursing Assistant certificate, which she had funded with student loans, she experienced health problems, and also had to care for her dying father. She was unable to work, and applied for disability benefits. She received a forbearance on her federal student loans, but not for her private student loans. Ms. Robertson made payments when she was able. However, payments did not stop the calls. In total, Navient called Ms. Robertson a total of 667 times, and called 522 times after she told them to stop calling. Navient would call back the same day even when Ms. Robertson told the collection agent that she would not have any money to pay until the following month.
2. *Gold v. Ocwen Loan Servicing, L.L.C.*[30] The plaintiff consented to being contacted about his mortgage debt, and answered several collection calls, but then asked for the calls to stop. However, the servicer called his cell phone at least 1,281 times between April 2, 2011 and March 27, 2014, despite repeated requests to stop.
3. *Montegna v. Ocwen Loan Servicing, L.L.C.*[31] The servicer called the plaintiff on his cell phone at least 234 times, even after he requested that the calls stop.
4. *Todd v. Citibank.*[32] Some time in January 2016, the bank began calling the plaintiff's cell phone. The 350 calls were often made twice a day, even after repeated requests to stop calling.[33]
5. *Critchlow v. Sterling Jewelers Inc.* (aka Jared).[34] The complaint alleges that Jared robocalled Mr. Critchlow more than 300 times, several times a day and on back-to-back days, even after he begged for the calls to stop, saying he simply did not have the money to pay the debt. The case was settled with a confidentiality agreement.

Most of these cases are settled, and in return for the settlement consumers are generally required to sign **confidentiality clauses** that prohibit them and their lawyers from disclosing the details of the settlements. These confidentiality clauses prevent reviewing courts from evaluating the repeated and persistent nature of the robocallers' behavior. By suppressing that information,

---

[29] Case No. 8:17-cv-01077 (M.D. Fla. filed May 8, 2017).

[30] 2017 WL 6342575 (E.D. Mich. Dec. 12, 2017).

[31] 2017 WL 4680168 (S.D. Cal. Oct. 18, 2017).

[32] 2017 WL 1502796 (D.N.J. Apr. 26, 2017).

[33] *Id.* at *8.

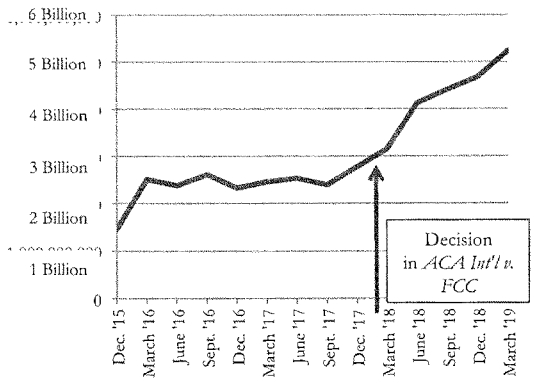
[34] Case No. 8:18-cv-00096 (M.D. Fla. filed Jan. 12, 2018).

robocallers are more likely to evade the TCPA's treble damages provision for knowing or willful violations.

III. Why Are the Calls Increasing?

A significant reason for the escalation in robocalls is that many robocallers are anticipating a caller-friendly response to the many requests they have submitted to the FCC to *loosen* restrictions on robocalls. This is evidenced by the spike in calls that occurred right after last year's decision in March 2018 by the D.C. Circuit Court in *ACA International v. F.C.C.*[35] That decision set aside a 2015 FCC order[36] on the question of what calling technology is included in the definition of an automatic telephone dialing system (ATDS),[37] and raised the specter that the term might be interpreted not to cover the autodialing systems that are currently used to deluge cell phones with unwanted calls.

Increase in Robocalls December 2015 through March 2019



The calling industry's response to this decision is perfectly illustrated by the petition to the FCC filed by the U.S. Chamber Institute for Legal Reform (U.S. Chamber),[38] joined by 16 major

---

[35] 885 F.3d 687 (D.C. Cir. 2018)

[36] *In re* Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, CG Docket No. 02-278, Report and Order, 30 FCC Rcd. 7961(F.C.C. July 10, 2015) [hereinafter 2015 Order].

[37] 47 U.S.C. § 227(a)(1).

[38] *In re* Rules & Regulations Implementing the Telephone Consumer Protection Act of 1991, U.S. Chamber Institute for Legal Reform, Petition for Declaratory Ruling, CG Docket No. 02-278 (filed May 3, 2018), *available at* https://ecfsapi.fcc.gov/file/105112489220171/18050803-5.pdf.

national industries,[39] to *loosen* restrictions on robocalls. **It is essential to understand, that if the request of the U.S. Chamber were to be granted, the scourge of robocalls will skyrocket.**

Additionally, losing defendants in judicial actions often seek protection from the FCC by asking for retroactive waivers for the liability they face after courts have found that they have made millions of robocalls without consent. And there are dozens of petitions currently pending at the FCC asking for special interpretations or exemptions, which seek to allow industries to ignore the basic rule of the TCPA that express consent must be provided before automated calls can be made to our cell phones. Allowing waivers and exemptions undermines compliance, and leads to increased unwanted robocalls. If the FCC rules the wrong way on these pending TCPA issues, Section 2 of H.R. 946 is essential.

IV. H.R. 946 is Needed to Protect Consumers.

Passage of H.R. 946 would create a powerful tool that will stop most unwanted robocalls in the United States. Congress should pass the entire bill, despite the robocallers' objections. Passage will save our telephone system. Each section of H.R. 946 accomplishes an important objective, responding to a different facet of the robocalling problem. Section 2 of H.R. 946 amends the TCPA in ways that are particularly important to consumers. While the current language in the TCPA already clearly permits the FCC to correctly interpret the TCPA to protect consumers from unwanted robocalls, passage of this section will ensure that consumers remain protected, regardless of potentially incorrect interpretations of the current provisions by the FCC.

Following is a section-by-section analysis of H.R. 946, illustrating the need for each provision, along with recommendations on behalf of consumers to protect all telephones from robocalls.

A. TCPA Covered Autodialers Include Systems that Call From Stored Lists--Section 2(a).

In its current form, the TCPA defines an ATDS as equipment that "has the capacity—(A) to store or produce telephone numbers to be called, using a random or sequential number generator; and (B) to dial such numbers."[40] In our view, and the view of a number of courts,[41] the current definition

[39] These industries include: ACA International, American Association of Healthcare Administrative Management, American Bankers Association, American Financial Services Association, Consumer Bankers Association, Consumer Mortgage Coalition, Credit Union National Association, Edison Electric Institute, Electronic Transactions Association, Financial Services Roundtable, Insights Association, Mortgage Bankers Association, National Association of Federally-Insured Credit Unions, National Association of Mutual Insurance Companies, Restaurant Law Center, and Student Loan Servicing Alliance.

[40] 47 U.S.C § 227(a)(1).

in the TCPA encompasses both systems that store numbers and dial them automatically, and systems that generate numbers and dial them automatically, and only the latter must use a random or sequential number generator to be covered. Other courts, however, take the position that a system must use "a random or sequential number generator" to qualify as a covered ATDS under the TCPA.[42] As described above, much of corporate America is applying heavy pressure on the FCC (and the courts) to interpret the TCPA's definition of "automatic telephone dialing system" (ATDS or "autodialer") narrowly, which would result in an effective nullification of the law's prohibition against autodialed calls and texts to cell phones without the called party's consent.

The issue is of great importance, because robodialing and robotexting technology is what enables so many billions of calls to be made every year. Yet many of the calling systems in use today do not call numbers randomly. Instead, they are "predictive dialers" that generate call lists from a database of numbers, and then robodial or robotext those numbers. For example, a telemarketer may purchase a list of consumers who have proven to be easy marks in the past; a debt collector may call numbers believed to belong to debtors; or a seller may buy a list of consumers who are believed to be interested in a certain type of product. If the definition of ATDS were interpreted as requested by the U.S. Chamber and other industries, the meaning would be so narrow that it would not apply to dialing systems that automatically dial from lists—those systems that are in use today—and there would be no way to stop this robocall onslaught.

The Third Circuit's decision in *Dominguez v. Yahoo, Inc.*[43] is an example of an interpretation of an ATDS that dangerously undermines the scope of the TCPA. In that case, Yahoo's completely

---

[41] Marks v. Crunch San Diego, L.L.C., 904 F.3d 1041 (9th Cir. 2018). *Accord* Evans v. Pa. Higher Educ. Assistance Agency, 2018 WL 6362637 (N.D. Ga. Oct. 11, 2018). *See also* Getz v. DirecTV, L.L.C., 359 F. Supp. 3d 1222 (S.D. Fla. 2019); Adams v. Ocwen Loan Servicing, L.L.C., ___ F. Supp. 3d ___, 2018 WL 6488062 (S.D. Fla. Oct. 29, 2018); Davis v. Diversified Consultants Inc., 36 F. Supp. 3d 217 (D. Mass. 2014); Echevvaria v. Diversified Consultants, Inc., 2014 WL 929275 (S.D.N.Y. Feb. 28, 2014), *adopted by* 2014 WL 12783200 (S.D.N.Y. Apr. 22, 2014).

[42] *See, e.g.,* Pinkus v. Sirius XM Radio, Inc., 319 F. Supp. 3d 927 (N.D. Ill. 2018). *Accord* Thompson-Harbach v. USAA Fed. Sav. Bank, 359 F. Supp. 3d 606 (N.D. Iowa Jan. 9, 2019). *See also* Johnson v. Yahoo!, Inc., 346 F. Supp. 3d 1159 (N.D. Ill. 2018); Gary v. Trueblue, Inc., 346 F. Supp. 3d 1040 (E.D. Mich. 2018).

[43] 894 F.3d 116 (3d Cir. 2018). Two other cases of uncontrolled technology resulting in a deluge of unwanted robocalls or texts are *Gonzalez-Pagan v. Redwood Capital Group* and *Schuster v. Uber Technologies, Inc.* In *Gonzalez-Pagan v. Redwood Capital Group*, a local developer called Mr. Gonzalez-Pagan approximately 5,000 times for years, often making more than 50 calls a day on back-to-back days, even though Mr. Gonzalez-Pagan owed nothing to the developer and had no idea how it put his cell number in its robodialing campaign. The calls continued even after Mr. Gonzalez-Pagan drove to the defendant's apartment complex and begged for the calls to stop. Over 500 calls were made even after the lawsuit was filed in federal court. Case No. 8:2017-cv-02184 (M.D. Fla.

automated text messaging system sent 27,809 unwanted text messages to one consumer.[44] The previous owner of the number had subscribed to an email-notification service offered by Yahoo, which sent a text message to the former owner's phone number every time an email was sent to the former owner's linked Yahoo email account. The consumer tried to halt the messages by replying "stop" and "help" to some texts. When he asked Yahoo's customer service for help, he was told that the company could not stop the messages, and that as far as Yahoo was concerned the number would always belong to the previous owner. The consumer then sought help from the FCC. In a three-way call with the consumer and Yahoo, the FCC tried to convince Yahoo to stop the messages, but was similarly unsuccessful. After receiving 27,809 text messages from a machine over 17 months, the consumer brought suit under the TCPA. Only after the case was filed did the messages finally stop.[45] Alarmingly, the Third Circuit ruled that tbe system was not an ATDS because the consumer did not prove that it had the present capacity to generate random or sequential numbers. This ruling, if accepted by other courts or the FCC, would leave every cell phone in America vulnerable to the same deluge of unstoppable text messages.

The issue of how to define an ATDS is currently pending at the FCC. The language in Section 2(a) would ensure that the dialers currently in use to make automated calls and texts are covered by the TCPA's protections.

Action Requested: Section 2(a) should be passed because it resolves this issue by clarifying that TCPA-covered calls are those made "using equipment that makes a series of calls to stored telephone numbers, including numbers stored on a list, . . ."

B. Covered Autodialers Include Systems Designed to *Evade* TCPA Coverage--Section 2(a).

Perhaps the most brazen attempt to evade the TCPA's protections against autodialed calls to cell phones is clicker-agent calling systems. These systems are entirely automated, but insert a human "clicker agent" into the process. These human clicking agents do not participate in the calls, and simply have the job of repeatedly clicking a single computer button, which sends telephone numbers on an already-created list to an automated dialer in an another locale. The seller then claims that the insertion of this human as an automaton means

---

filed Sept. 21, 2017). In *Schuster v. Uber Technologies, Inc.*, Mr. Shuster sued Uber for sending 1,050 text messages without consent and despite repeated requests to cease. Case No. 8:18-cv-02389 (M.D. Fla. filed Sept. 27, 2018).

[44] Dominguez v. Yahoo, Inc., 629 Fed. Appx. 369, 371 (3d Cir. 2015).

[45] *Id.* at 370–71.

that the calls are not governed by the TCPA, so the calls can be made without consent and the called party has no way to stop them.[46]

If this position were accepted, it would profoundly impair our ability to control unwanted calls to our cell phones. For example, a single seller, Hilton Grand Vacations Co., used a clicker-agent system to make *56 million calls* to cell phones to sell vacation packages, and then claimed that they were not made with an ATDS and thus that the TCPA did not apply and no consent was required.[47] And that is just one company. Allowing clicker-agent calls to evade the TCPA would amount to an invitation to every telemarketer—both those pushing overt scams and those making less shady, but equally intrusive, calls—to make millions of calls without consent. Clicker-agent systems not only result in mass unwanted automated calls to cell phones, but also produce the same problems of dropped calls and delays after answering the phone that calls made by all autodialers produce.[48]

Consumer groups have asked the FCC to rule on these evasion efforts and clarify that systems that use human clicker agents to process phone numbers that are then automatically dialed are covered by the TCPA. However, the FCC has not yet issued a response.

Section 2(a) would assure that systems that are highly automated but developed just to evade coverage—and thus avoid the TCPA's requirement for prior express consent—would clearly be covered.

Action Requested: Section 2(a) should be passed because it resolves this issue by exempting only equipment "that the caller demonstrates requires substantial additional human intervention to dial or place a call after a human initiates the series of calls; …"

C. Ensuring that Consumers Can Revoke Consent—Section 2(b).

The TCPA was written explicitly to protect Americans from the "scourge of robocalls" by giving consumers control over whether they receive robocalls. Congress did so by giving consumers

---

[46] These clicker-agent systems are quite distinct from systems in which there is actually a human that makes the calls. In these systems, the human agent caller brings up the information about a particular consumer on a screen, and then the agent makes a conscious decision to call that consumer and presses a button and the call is made. The human is involved in deciding whether and when to make the call, and the call is made only when the human presses the button to make it. Systems like this are typically called "preview dialers."

[47] Glasser v. Hilton Grand Vacations Co., L.L.C., 341 F. Supp. 3d 1305 (M.D. Fla. 2018), *appeal to 11th Circuit pending.*

[48] According to the record in the case, Hilton's documents included an illustration of the two systems side by side. Doc. 104-7, at 2. The two systems appear to be identical *except for* the addition of the superfluous clicker agent for the TCPA-covered calls.

the right to chose whether to consent—and implicitly to withhold or revoke that consent—to automated calls.

The calling industry has asked the FCC to issue a ruling that consent provided as part of a contract cannot be unilaterally revoked by the consumer.[49] Such a ruling would effectively eradicate the TCPA's requirement for express consent for automated calls.

The D.C. Circuit's decision in *ACA International* confirmed the FCC's conclusion in its 2015 Order[50] that consumers have the right to revoke consent.[51] However, the *ACA International* court did not take a position on whether the FCC had authority to determine that revocation of contractually provided consent might be limited by contract, because the issue was not before the court.[52]

Most of the automated calls about which consumers complain are either telemarketing calls or debt collection calls. For calls made by debt collectors, the FCC has explicitly allowed consent to be presumed whenever consent was provided in the original credit contract with the creditor or the seller. But those contracts are adhesion contracts, in which consumers have no bargaining power and no ability to change the terms. So it is already a stretch for the FCC to have said that consent for debt collection calls—which is required by statute to be *express*—can be *implied* when a consumer gives her telephone number to open a charge account in a store. Providing a telephone number when applying for credit hardly constitutes express consent to be contacted months or years later by a debt collector.[53] Courts have stretched the notion of express consent even farther by holding that consent can be transferred from the original creditor to a debt buyer, and then from the debt buyer to a collector it hires.[54]

It would be a true overextension for the FCC to take the next step down the road to unlimited automated calls and hold that, once a consumer has provided her phone number in a contract, she

---

[49] *See, e.g.*, Comments of U.S. Chamber Institute for Legal Reform, *In re* Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, CG Docket Nos. 02-278 and 18-152, at 21, 27 (filed June 13, 2018), *available at* https://ecfsapi.fcc.gov/file/1061348977655/ILR-US%20Chamber%20TCPA%20Public%20Notice%20Comments.pdf.

[50] 2015 Order at 7993.

[51] ACA International v. F.C.C., 885 F.3d 687, 709 (D.C. Cir. 2018).

[52] *Id.* at 710 (emphasis added; citation omitted).

[53] "[P]ersons who knowingly release their phone numbers have in effect given their invitation or permission to be called at the number which they have given, absent instructions to the contrary." *In re* Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, CG Docket No. 92-90, Report and Order, 7 F.C.C. Rcd. 8752, 8769 ¶ 31 (Oct. 16, 1992).

[54] *See* Selby v. LVNV Funding, L.L.C., 2016 WL 6677928, at *8 (S.D. Cal. June 22, 2016).

could never stop a debt collector's continuing automated calls by withdrawing that consent. One Second Circuit decision, *Reyes v. Lincoln Automotive Financial Services*,[55] erroneously holds that the consumer's consent is irrevocable when it is part of a binding contract. That decision fails to give appropriate weight to the FCC's 2015 Order ruling that, "[w]here the consumer gives prior express consent, the consumer may also revoke that consent."[56] The *Reyes* decision also mistakenly holds that no other Circuit had addressed the question, when in fact several other Circuits had upheld the consumer's right to revoke consent that was given in a contractual context.[57]

If revocation is not permitted, robocalls will be even more abusive and unstoppable. Debt collection callers comprise nineteen of the top twenty robocallers in the United States.[58] As detailed above, debt collection calls are among the top calls about which consumers complain. Often, debt collectors and creditors collecting their own debts are now routinely refusing to stop calling, despite pleas from consumers, and are instead arguing that the Second Circuit's *Reyes* decision applies to them and that consent cannot be revoked. We can only imagine the nightmare scenario that will impact tens of millions of people across the U.S. if the FCC rules that consent granted by contract cannot be revoked.

Section 2(b) will ensure that when a consumer says to a robocaller "stop calling," the caller will know that it must stop calling, or face pay statutory damages for calls made after the demand to stop was made.

Action Requested: Section 2(b) should be passed because it resolves this issue by clarifying that "prior express consent may be revoked at any time and in any reasonable manner, regardless of the context in which consent was provided."

D. Preventing Callers' Evasive Actions to Avoid TCPA Compliance—Section 2(c).

Robocallers—particularly the "legitimate businesses" that can actually be traced and called to account for their violations—go to great lengths to devise ways to bombard us with calls without our

---

[55] 861 F.3d 51, 58 (2d Cir. 2017).

[56] 2015 Order at 7996. *See* Ginwright v. Exeter Fin. Corp., 280 F. Supp. 3d 674, 683 (D. Md. 2017) (declining to follow *Reyes*; noting its inconsistency with FCC's ruling).

[57] *See* Gager v. Dell Fin. Servs., L.L.C., 727 F.3d 265 (3d Cir. 2013) (consent provided in application for credit). *See also* Schweitzer v. Comenity Bank, 866 F.3d 1273 (11th Cir. 2017) (consent provided in credit card application can be revoked, and consumer can revoke consent in part); Van Patten v. Vertical Fitness Grp., 847 F.3d 1037, 1047–49 (9th Cir. 2017) (consent provided in gym membership application); Osorio v. State Farm Bank, 746 F.3d 1242 (11th Cir. 2014) (consent provided in application for credit card, although the court allows that the *method* of revoking consent may be limited by the contract).

[58] *See* YouMail Robocall Index, *available at* https://robocallindex.com/ (last accessed Apr. 9, 2019).

consent yet evade liability. One strategy they use is deploying "lead generators" or "data brokers" to place the calls. On these calls from data brokers, once a consumer indicates an interest in the product being sold ("Press 2 now if you want to hear more about available health insurance in your area."), the broker passes along the consumer's information to the company selling the product. When the seller (who is paying the robocaller for the leads that result from the unwanted telemarketing calls) is sued, it typically defends by saying it did not know about, or is not responsible for, the TCPA violations committed by these independent third parties.[59]

Another strategy is to hire others to make the calls and then claim that the actual callers were independent contractors for whom the seller is not responsible. The seller may put a clause in its contract with the independent contractor that purports to require it to comply with the TCPA, and then claim that it can't possibly be held liable since the independent contractor promised to obey the law.

This ploy was outlined—and strongly disapproved of—in the case of *Krakauer v. Dish Network, L.L.C.*[60] Dish Network's telemarketers had made millions of illegal and unwanted calls to consumers,[61] and had persisted in doing so despite numerous complaints, and promises made to 46 state attorneys general. The court adjudicating the case found that the independent contractors were agents of Dish Network, and that Dish was vicariously liable for the calls made by the independent

---

[59] *See, e.g.,* McCurley v. Royal Seas Cruises, Inc., 2019 WL 1383804 (S.D. Cal. Mar. 27, 2019) (defendant claimed it was not responsible for the 634 million calls made by the lead generator); Aranda v. Caribbean Cruise Line, Inc. 179 F. Supp. 3d 817 (N.D. Ill. 2016) (defendant claimed it was not responsible for millions of calls made by third party.); Hossfeld v. Gov't Employees Ins. Co., 88 F. Supp. 3d 504 (D. Md. 2015) (GEICO claimed it was not responsible for calls made third parties and transferred to GEICO); Smith v. State Farm Mut. Auto. Ins. Co. 2015 WL 13658072 (N.D. Ill. Jan. 13, 2015) (over 80,000 consumers called; defendant denied responsibility for calls made by third party).

[60] 311 F.R.D. 384 (N.D.N.C. 2015)

[61] United States v. Dish Network, L.L.C., 75 F. Supp. 3d 942, 1022 (C.D. Ill. 2014) ("[T]he United States established in Count I that Dish and the Telemarketing Vendors made millions of outbound telemarketing calls to telephone numbers on the Registry as part of this nationwide pattern and practice of telemarketing."), *opinion amended on reconsideration sub nom.* United States v. Dish Network, L.L.C., 80 F. Supp. 3d 914 (C.D. Ill. 2015), and *opinion vacated in part on reconsideration sub nom.* United States v. Dish Network, L.L.C., 80 F. Supp. 3d 917 (C.D. Ill. 2015).

contractors to sell Dish products.[62] Yet sellers still commonly raise this subterfuge in case after case as a means of avoiding liability for the illegal calls made on their behalf.[63]

Yet another tactic of some robocallers is to use "soundboard technology" to make telemarketing calls to consumers, for example selling cruises and home security systems. This technology allows telemarketers to play prerecorded clips to consumers who answer the phone. A single telemarketer will often conduct more than one call simultaneously, playing prerecorded clips selected to appear to be responsive to the consumer and to keep the consumer on the phone. In one case, NorthStar Alarm Services[64] was responsible for over 75 million soundboard calls to sell home security systems to people who had no prior relationship with the company; the telephone numbers were all purchased from a data seller.[65] The telemarketer used Caller ID spoofing to display bogus telephone numbers to consumers. Because the calls were made with soundboard technology, which uses audio snippets of a prerecorded voice in calls to consumers, NorthStar claimed these calls should not be governed by the explicit requirements and limitations imposed on calls with a prerecorded voice under the TCPA.[66] Indeed, after the court allowed the case to proceed, NorthStar petitioned the FCC to hold that calls with audio snippets of a prerecorded voice should not be treated as calls with a prerecorded voice.[67] That petition is still pending.

There are many dozens of these cases, cumulatively involving hundreds of millions of calls to consumers, all defended by American businesses trying to sell their goods or services through robocalling our telephones. When sued for TCPA violations, these telemarketers come up with a range of excuses for why they should not be held liable for their violations. The Appendix provides a

---

[62] *See* Krakauer v. Dish Network L.L.C., 2017 WL 2242952, at *3 (M.D.N.C. May 22, 2017 ("The OE Retailers collectively generated hundreds of millions of dollars a year in revenue for Dish. Dish's contract with SSN gave it virtually unlimited rights to monitor and control SSN's telemarketing. In a settlement agreement with dozens of state attorneys general in 2009, Dish confirmed that it had this power over all of its marketers.").

[63] *See, e.g.*, Bakov v. Consol. World Travel, Inc., 2019 WL 1294659 (N.D. Ill. Mar. 21, 2019) (defendant claimed it was not responsible for the millions of calls made by an agent using soundboard technology); Armstrong v. Investor's Business Daily, Inc., 2018 WL 6787049 (C.D. Cal. Dec. 21, 2018) (defendant claimed it had no vicarious liability for calls by third parties).

[64] Braver v. NorthStar Alarm Servs., L.L.C., 329 F.R.D. 320 (W.D. Okla. 2018) (defendant claimed that soundboard technology did not use a "prerecorded voice" as defined by the TCPA).

[65] Braver v. NorthStar Alarm Servs., 15-cv-383, Doc. 42 (W.D. Okla.).

[66] 47 U.S.C. § 227.

[67] NorthStar Alarm Services, Petition for Expedited Ruling Clarifying 47 U.S.C. § 227(b)(1)(B) of the Telephone Consumer Protection Act (filed Jan. 2, 2019), *available at* https://ecfsapi.fcc.gov/file/10103290733918/NorthStar%20FCC%20Petition.pdf.

list of just 33 of them, along with the excuses the callers made to evade responsibility for their unwanted and illegal calls.

While the FCC has ruled appropriately on some of these issues, the language of Section 2(c) will unambiguously direct the FCC to ensure that no evasions are permitted.

Action Requested: Section 2(c) should be passed because it addresses these attempted evasions by requiring the FCC to issue regulations that "prevent circumvention or evasion . . . ."

E. Limiting Exemptions—Section 3.

Section 3 sets a number of appropriate consumer protection limits on any exercise of the FCC's authority to make exemptions from the TCPA's requirements. It relates to two provisions of the TCPA that give the FCC exemption authority. First, it relates to section 227(b)(2)(B), which allows the FCC to exempt non-commercial calls from the restrictions on prerecorded calls to land lines, and calls for a commercial purpose if they do not include advertisements and do not adversely affect the privacy rights the TCPA is intended to protect. Second, it relates to section 227(b)(2)(C), which allows the FCC to exempt free-to-end-user calls from the restrictions on prerecorded or autodialed calls to cell phones—again, as long as the calls do not adversely affect the privacy rights the TCPA is intended to protect.

Section 3 would require any such exemptions to include requirements regarding the classes or categories of parties that may make such calls and the parties to whom such calls may be made; the purposes for which such calls may be made; and the number of calls that a calling party may make to a particular called party. It would also require any robocaller making use of such an exemption to give the called party an opt-out mechanism, with which the caller must abide.

We thank the drafters of this bill for including limits on exemptions. Like the drafters, we are concerned about the constant stream of exemption requests from robocallers to the FCC. Even though the FCC's exemption authority is not unbounded, and is limited by the TCPA to certain enumerated circumstances, these exemption requests could do a great deal of harm. If the FCC were to grant even a small portion of the exemption requests it receives, it would riddle the TCPA with holes.

Section 3's list of requirements that any exemptions must meet will also help ensure that any exemptions are crafted to achieve their purpose with the least possible negative effect on the privacy interests that the TCPA is intended to protect. For example, section 3 would not allow the FCC to grant an exemption that allowed unlimited unwanted calls. Instead, any exemption would have to include a limit on the number of calls that the robocaller could make to a particular consumer.

Section 3 would also require any exemption to give the consumer a conspicuous opt-out mechanism by which the consumer could require the robocaller to stop calling.

Requirements like these are important not just as a policy matter. Last week, the Fourth Circuit issued a decision, *American Association of Political Consultants, Inc. v. Federal Communications Commission,*[68] holding that the 2015 amendment to the TCPA that created an exemption for calls to collect government debt was unconstitutional because it created different rules for speech based on the content of the speech. A major element in the court's conclusion was its view that the exemption was not narrowly tailored.

The time for the parties to petition for rehearing has not passed, and several lower courts have taken a different view,[69] so this decision cannot be considered the last word on the question. Nonetheless, it highlights the importance of narrowly framing any exemptions so that they will not interfere with the privacy protection purposes of the TCPA.

We also recommend that the Committee consider whether to rework the section's language so that any exemption must articulate the purposes for which the exempted calls may be made. The recent Fourth Circuit decision held that the exemption for calls to collect government debts was content-based and therefore triggered First Amendment scrutiny. It might be better simply to require that any exemption identify clearly the calls or callers that are exempted.

Action Requested: Section 3 should be passed to place limits on the FCC's exemption authority.

F. Dealing Effectively with Wrong Number Calls—Section 4.

Section 4(a) requires the establishment of a reassigned number database to provide a mechanism for callers to determine whether the numbers they want to call are still used by the persons from whom they obtained consent. FCC Chairman Pai has already established a reassigned number database,[70] and he deserves substantial credit for doing so. Further, although the FCC did

---

[68] ___ F.3d ___, 2019 WL 1780961 (4th Cir. 2019).

[69] Gallion v. Charter Commc'ns, Inc., 287 F. Supp. 3d 920 (C.D. Cal. 2018); Greenley v. Laborers' Int'l Union of N. Am., 271 F. Supp. 3d 1128 (D. Minn. 2017) (emergency and government debt exceptions are content-based, but serve a compelling governmental interest so are constitutional); Holt v. Facebook, Inc., 240 F. Supp. 3d 1021, 1032–1034 (N.D. Cal. 2017) (neither government debt nor emergency exception renders TCPA unconstitutional); Brickman v. Facebook, Inc., 230 F. Supp. 3d 1036 (N.D. Cal. 2017) (TCPA withstands strict scrutiny despite exceptions for emergency calls and government debt collection calls), *motion to certify interlocutory appeal granted*, 2017 WL 1508719 (N.D. Cal. Apr. 27, 2017); Mejia v. Time Warner Cable Inc., 2017 WL 3278926 (S.D.N.Y. Aug. 1, 2017).

[70] *In re* Advanced Methods to Target and Eliminate Unlawful Robocalls, CG Docket No. 17-59, Second Report and Order, FCC 18-177 (Rel. Dec. 13, 2018), *available at*

adopt a safe harbor for callers that relied on information in the database to make wrong number calls, it appropriately limited the safe harbor to those callers that *properly used* the database and relied on it to make the call that turned out to be to a wrong number.[71] Section 4(a) will endorse this initiative and codify it into statute, protecting it from challenges that the calling industry might mount.

Section 4(b) also deals with the problem of wrong number calls by addressing the—rather absurd—insistence of many robocallers that the term "called party," as used throughout the TCPA, means the person the caller "intended to call," rather than the person actually reached.[72] The FCC is considering this very issue in a pending proceeding.[73] Passage of Section 4(b) will ensure that the FCC does not adopt the robocallers' illogical and dangerous interpretation, which would leave us unprotected from unwanted robocalls made by callers who would then have no incentive to ensure that they were only calling the people who had consented to be called.

It is important to note that the litigation around reassigned number calls is caused by *repeated and unstoppable* calls to the wrong number, not just one or two mistaken calls. Consumers are begging callers to stop the calls, and it is only when they don't that the consumer must resort to seeking legal advice to stop the calls and obtain legal redress. Some recent examples—from many similar cases—include:

1. *Allen v. JPMorgan Chase.*[74] Sheila Allen received about 80 calls from Chase regarding an auto loan that was not hers. The calls continued despite repeated requests that they stop.

2. *Lebo v. Navient.*[75] Zachary Lebo received 100 calls from Navient over two months for a "Justine Sulia," sometimes as many as five calls a day. He had never given permission for

---

https://consumerfinancialserviceslaw.us/files/2018/12/FCC-18-177A1-Final-Report-and-Order-on-Reassigned-Number-Database.pdf.

[71] *Id.* at 20, ¶¶ 55, 56.

[72] *See, e.g.,* Soppet v. Enhanced Recovery Co., L.L.C., 679 F.3d 637, 640 (7th Cir. 2012) ("The phrase 'intended recipient' does not appear anywhere in § 227, so what justification could there be for equating 'called party' with 'intended recipient of the call'?"); Moore v. Dish Network L.L.C., 57 F. Supp. 3d 639, 648-649 (N.D. W. Va. 2014) (rejecting argument that only "called party" has standing; "No portion of § 227 states that only the intended recipient of a call can recover under it."); Swope v. Credit Mgmt., L.P., 2013 WL 607830, at *3 (E.D. Mo. Feb. 19, 2013) (finding no support for the argument that only a "called party" has standing; "Furthermore, even if the TCPA limits standing to 'called parties' the plaintiff qualifies as a called party under the facts of this case. Numerous courts that have considered this issue have held a party to be a 'called party' if the defendant intended to call the individual's number, and that individual was the regular user and carrier of the phone.").

[73] *See* Public Notice, Federal Communications Commission, Consumer and Governmental Affairs Bureau Seeks Comments on Interpretation of the Telephone Consumer Protection Act in Light of the D.C. Circuit's ACA International Decision, CG Docket Nos. 18-152 and 02-278 (Rel. May 14, 2018), *available at* https://ecfsapi.fcc.gov/file/0514497027768/DA-18-493A1.pdf.

[74] Case No. 1:13-cv-08285 (N.D. Ill. filed Nov. 18, 2013).

Navient to call him, and he revoked permission over the phone; yet the calls continued.

3. *Waite v. Diversified Consultants.*[76] Patricia Waite and her daughter Heather received about 166 calls from Diversified Consultants for "Marcy Rodriguez," whom neither of them knows. Diversified continued calling multiple times a day despite being told that it had a wrong number.

4. *Moseby v. Navient Solutions,* Inc.[77] Terrance Moseby received dozens of calls from Navient for a "Joshua Morris" or "Andrea." Mr. Moseby has never had any relationship with Navient or either of these people. He told Navient that it had the wrong number, but the calls continued.

As these cases illustrate, to protect consumers it is imperative that the pressure be maintained on callers to ensure that they are calling the correct number: the number that belongs to the consumer from whom they have consent to call. Mistakes do happen. But these lawsuits are not about a single mistake. These lawsuits are about callers who persist in calling numbers they have repeatedly been told do not belong to the person who provided consent. These cases are brought against callers that clearly did not have enough of a financial incentive to make sure that they stopped calling—and harassing—consumers with whom they had no relationship, who had not provided consent, and who begged the callers to stop the calls.

The robocallers' argument that "called party" should be interpreted to mean the person the robocaller "intended" to call, rather than the person who was actually called, is weak. It was rejected by the Seventh Circuit *in Soppet v. Enhanced Recovery Co.*,[78] in an opinion that the D.C. Circuit found "persuasive."[79] The term "called party" is used in several other places in the statute where it can be interpreted only to mean the party actually called, and it would go against the rules of statutory construction, as well as common sense, to hold that the term means one thing in one part of a statute and something else in another part of the same statute. Yet the FCC appears to be considering the adoption of exactly that interpretation.[80]

---

[75] Case No. 2:17-cv-00154 (D. Wyo. filed Sept. 15, 2017).

[76] Case No. 5:13-cv-00491 (M.D. Fla. filed Oct. 7, 2013).

[77] Case No. 4:16-cv-00654 (E.D. Ark. filed Sept. 9, 2016).

[78] 679 F.3d 637 (7th Cir. 2012)

[79] ACA International v. F.C.C., 885 F.3d 687, 706 (D.C. Cir. 2018).

[80] *See* Public Notice, Federal Communications Commission, Consumer and Governmental Affairs Bureau Seeks Comments on Interpretation of the Telephone Consumer Protection Act in Light of the D.C. Circuit's ACA International Decision, CG Docket Nos. 18-152 and 02-278, at 3-4 (Rel. May 14, 2018), *available at* https://ecfsapi.fcc.gov/file/0514497027768/DA-18-493A1.pdf.

Callers' exposure to liability for making wrong number calls provides an essential incentive for them to spend the time and money to limit wrong number calls. Once the reassigned number database is operational, using it correctly will be the best way to ensure that callers are not calling reassigned numbers. If the definition of "called party" were interpreted to mean "intended recipient," there would be no reason for callers to use the database, as they would not face any liability for calls to reassigned numbers whether or not they used it.

Action Requested: Section 4(b) should be passed to ensure that the definition of "called party" can be interpreted only to mean the party actually called.

G. Improving Enforcement Mechanisms—Section 5.

Section 5 of H.R. 946 provides enhanced enforcement mechanisms for violations of the TCPA by extending the statute of limitations and reducing some of the requirements for actions brought by the FCC in prosecuting violations of the TCPA.

It is important that the FCC be able to bring effective enforcement actions against violators of the TCPA, largely because without enforcement there is little deterrence. Unfortunately, FCC enforcement does not accomplish this goal. According to a recent article in the Wall Street Journal, the FCC has collected only $6,790 in fines against violators of the TCPA.[81]

Individual actions are essential for providing redress to individual consumers, but provide little deterrent effect on the callers. These callers simply pay up and repeat the pattern with other victims. Obviously, routinely violating the law and paying damages to the few consumers who actually file actions is more financially beneficial than complying with the law—else these robocallers would not keep repeating the pattern, as they are now doing. Moreover, TCPA litigation can be complicated and expensive, and the statute does not allow for the recovery of attorneys' fees, making individual claims about a small number of calls non-viable as a practical matter.

In contrast, private enforcement through class actions provides significant deterrence against illegal robocalls. The calling industry complains incessantly about the "nuisance class actions" brought by plaintiffs' attorneys, and cites these cases as a basis for requesting a variety of changes in the interpretation of TCPA terms. However, class actions drive compliance with the law and the FCC's

[81] Sarah Krouse, *The FCC Has Fined Robocallers $208 Million. It's Collected $6,790,* The Wall Street Journal, Mar. 28, 2019, *available at* https://www.wsj.com/articles/the-fcc-has-fined-robocallers-208-million-its-collected-6-790-11553770803. The article cites as a source for the analysis "records obtained by The Wall Street Journal through a Freedom of Information Act request."

rules. In addition to strengthening the FCC's enforcement tools, Congress should preserve and strengthen the ability of consumers themselves to enforce the TCPA.

Repeat violators of this 40-year-old law cry foul when forced to answer for their transgressions. Lost in the rhetoric is the fact that many of the same corporations are violating the same law while ignoring the same pleas for the calls to stop. It seems that corporations have made the business decision that ignoring the TCPA is more profitable than compliance. Even more troubling, the consumers who experienced these violations of federal law are then sworn to secrecy through confidentiality clauses and subject to liquidated damages of potentially thousands of dollars if they share their stories.

Because class actions cost the calling industry money when they are held accountable for failing to follow the simple requirements for obtaining consent before they make robocalls, callers are more likely to change their behavior to avoid being held liable in a class action case. As the federal district court judge noted in a telemarketing case against Dish Network involving millions of calls:

> [T]he legislative intent behind the TCPA supports the view that class action is the superior method of litigation. "[I]f the goal of the TCPA is to remove a 'scourge' from our society, it is unlikely that 'individual suits would deter large commercial entities as effectively as aggregated class actions and that individuals would be as motivated ... to sue in the absence of the class action vehicle.'"[82]

Indeed, in another opinion related to this case, the court recited the failure of the defendant to comply with its promise to government enforcers, explaining its rationale for awarding treble damages for the defendant's willful violations of the TCPA:

> The Court concludes that treble damages are appropriate here because of the need to deter Dish from future violations and the need to give appropriate weight to the scope of the violations. The evidence shows that Dish's TCPA compliance policy was decidedly two-faced. Its contract allowed it to monitor TCPA compliance, and it told forty-six state attorneys general that it would monitor and enforce marketer compliance, but in reality it never did anything more than attempt to find out what marketer had made a complained-about call. It never investigated whether a marketer actually violated the TCPA and it never followed up to see if marketers complied with general directions concerning TCPA compliance and or with specific do-not-call instructions about individual persons. Dish characterized people who pursued TCPA lawsuits not as canaries in the coal mine, but as "harvester" plaintiffs who were illegitimately seeking money from the company. The Compliance Agreement did not cause Dish to take the TCPA seriously, so significant damages are appropriate to emphasize the seriousness of such statutory violations and to deter Dish in the future.
> . . .

[82] Krakauer v. Dish Network L.L.C., 311 F.R.D. 384, 400 (M.D.N.C. 2015) (emphasis added; citation omitted).

> This case does not involve an inadvertent or occasional violation. It involves a sustained and ingrained practice of violating the law.
>
> Dish did not take seriously the promises it made to forty-six state attorneys general, repeatedly overlooked TCPA violations by SSN, and allowed SSN to make many thousands of calls on its behalf that violated the TCPA. Trebled damages are therefore appropriate.[83]

Most of the litigation under the TCPA relates to calls to cell phones, because violations trigger damages after the first call. However, these cases are costly and complex to litigate, requiring experts to opine on technical issues such as whether the caller used an ATDS, or to assist in determining the number of covered calls, as well as analyze issues of consent. Calls to landlines are much less protected. Private litigation should be encouraged and facilitated by the laws governing robocalls, by allowing courts to award attorneys' fees to successful plaintiffs.

Additionally, the routine violation of the Do Not Call Registry by telemarketers illegally calling our residential phones has been a significant reason that many people have abandoned their residential landlines. Senator Durbin is introducing a bill that remedies this problem by making damages for violations of the Do Not Call Registry on the same basis as those available for making illegal calls to cell phones.

Action Requested:

1) Section 5 of H.R. 946 should be passed;

2) The TCPA should be amended to make it easier for victims of unwanted robocalls to bring actions against callers who violate the TCPA, by allowing courts to award plaintiffs attorneys' fees; and

3) The TCPA should be amended to provide equivalent damages for violating the Do Not Call Registry as are provided for making illegal calls to cell phones.

H. Improving the Reliability of Caller ID—Sections 6 and 7.

To decide whether to answer the phone one must know who is calling. This requires that both the name displayed—if a name is displayed—and the phone number displayed be accurate. In this era of incessant robocalling, if we can't actually identify who the real caller is, we don't have good information about whether to answer the phone.

---

[83] Krakauer v. Dish Network L.L.C., 2017 WL 2242952, at *12–13 (M.D.N.C. May 22, 2017) (emphasis added; internal citations omitted.).

Currently the TCPA contains this provision dealing with Caller ID spoofing:

> (e) It shall be unlawful for any person within the United States, in connection with any telecommunications service or IP-enabled voice service, to cause any caller identification service to knowingly transmit misleading or inaccurate caller identification information with the intent to defraud, cause harm, or wrongfully obtain anything of value, unless such transmission is exempted pursuant to paragraph (3)(B).[84]

Sections 6 and 7 of H.R. 946 take important steps to improve Caller ID reliability. While these are important steps, they do not go far enough to fully address the problem of spoofing. First, under the current statutory language, which H.R. 946 does not change, spoofing is illegal *only* if done with the specified wrongful intent. This is a very difficult standard to prove. This law, even with the new language in H.R. 946, will not prevent telemarketers and debt collectors from spoofing phone numbers

Another problem, as outlined recently in an article in the New York Times, illustrates that even ensuring authentic Caller ID information will not fully address the problem of anonymous robocalls. When discussing the new Stir/Shaken protocol now being employed by some telephone providers—and which they will be required to use if S. 151[85] (known as the TRACED Act) is enacted—the article noted that:

> The new standard hasn't yet been rolled out, and there are already cheap and easy ways to circumvent it. Scammers who can't hide behind spoofed numbers can just buy real ones — for $1 a month or less — and make tens of thousands of calls from each of them.
>
> "Many such services today require only a credit card, so that a robocaller can easily acquire a number, use it for robocalls until the number makes its way onto too many blacklists to be useful and then pick a new one," said Henning Schulzrinne, a professor of computer science at Columbia University who was a chief technology officer at the F.C.C. from 2012 to 2014 and again in 2017.[86]

To deal with this additional threat to our ability to know who is calling us, the FCC should be required to determine additional means to ensure that telephone service providers be able to

---

[84] 42 U.S.C. § 227(e)(1) (emphasis added).

[85] This bill, sponsored by U.S. Sens. John Thune (R-S.D.) and Ed Markey (D-Mass.), is the Telephone Robocall Abuse Criminal Enforcement and Deterrence (TRACED) Act, S. 151.

[86] Tara Siegel Bernard, *Phone Companies Are Testing Tech to Catch Spam Calls. Let's Hope It Works.*, The New York Times, Apr. 26, 2019, *available at* https://www.nytimes.com/2019/04/26/your-money/robocalls-spam-calls.html.

identify who is using their system to place calls. These sections, as well as the TRACED Act[87] are good starts on the effort to authenticate Caller IDs, but it does not provide a mandate to address this additional threat posed by callers' ability to purchase untraceable phone numbers.

Action Requested:

1) Sections 6 and 7 of H.R. 946 should be clarified to mandate that the FCC require that the implementation of technological and other solutions to ensure that all robocallers are clearly identifiable and clearly traceable;

2) The TCPA should be amended specifically to prohibit the transmission of misleading or inaccurate caller ID information, except in limited circumstances necessary for law enforcement or the protection of the caller (while still permitting caller ID suppression altogether); and

3) Caller ID requirements should be clarified so that telephone service providers are required to prevent the connection of calls (or texts) for which accurate Caller ID information is not attached to a known customer whose name and address matches the originating call provider's information for that number.

V. Consumer Support for Other Pending Anti-Robocall Bills.

In recognition of extent of the current robocall crisis, there are several other excellent bills pending in the House to deal with unwanted robocalls. Among those others, and without limitation, we strongly support the following:

1. H.R. 1421, the "HANGUP Act, the "Help Americans Never Get Unwanted Phone calls (HANGUP) Act of 2019." The HANGUP Act would rescind section 301 of the Bipartisan Budget Act of 2015 exempting calls "made solely to collect a debt owed to or guaranteed by the United States" from the TCPA so that these debt collectors did not have to get consent from consumers before calling.

2. H.R. 2355, the "Regulatory Oversight Barring Obnoxious (ROBO) Calls and Texts Act." Among other things, this bill would require the FCC to implement regulations to compel carriers to adopt technological standards to prevent robocalls and periodically update those regulations.

3. H.R. 2298, the "Repeated Objectionable Bothering Of Consumers On Phones Act." Among other things, this bill would mandate call blocking of illegal robocalls and hold telephone service providers liable for failing in their obligations under the bill.

Thank you for caring about the concerns of consumers. I am available to answer any questions.

---

[87] S. 151.

Respectfully submitted:

Margot Saunders
Senior Counsel
National Consumer Law Center

Appendix
Illustrative Recent Telemarketing Cases
Against American Businesses -- with their Stated Defenses

1. Pine v. A Place for Mom, Inc., 2019 WL 1531689 (W.D. Wash. Apr. 9, 2019) (Defendant claimed it calls were not made on an ATDS).

2. Bennett v. GoDaddy.com L.L.C., 2019 WL 1552911 (D. Ariz. Apr. 8, 2019) (Defendant claimed the telemarketing calls to cell phones were not covered because the cell phones were used for business purposes).

3. McCurley v. Royal Seas Cruises, Inc., 2019 WL 1383804 (S.D. Cal. Mar. 27, 2019) (Defendant claimed it was not responsible for the 634 million calls made by the lead generator.).

4. Wakefield v. ViSalus, Inc., 2019 WL 1411127 (D. Or. Mar. 27, 2019) (Defendant claimed it had consent and was not responsible for the 1,850,436 calls made to consumers).

5. Bakov v. Consol. World Travel, Inc., 2019 WL 1294659 (N.D. Ill. Mar. 21, 2019) (Defendant claimed it was not responsible for the millions of calls made by an agent using soundboard technology).

6. Parker v. Universal Pictures, 2019 WL 1521708 (M.D. Fla. Feb. 28, 2019) (Text marketing campaign for a movie, with over 500,000 calls).

7. Getz v. DirecTV, L.L.C., 359 F. Supp. 3d 1222 (S.D. Fla. Feb. 20, 2019) (DirecTV sent thousands of text messages to consumers, defendant claimed text messages were not sent with ATDS).

8. Katz v. Liberty Power Corp., L.L.C, 2019 WL 957129 (D. Mass. Feb. 27, 2019) (Liberty Power called hundreds of consumers, claimed the TCPA is unconstitutional).

9. Armstrong v. Investor's Business Daily, Inc., 2018 WL 6787049 (C.D. Cal. Dec. 21, 2018) (479,000 unique mobile numbers contacted, defendant claimed it had no vicarious liability for calls by third parties).

10. Pedro-Salcedo v. Haagen-Dazs Shoppe Co., Inc., 2017 WL 4536422 (N.D. Cal. Dec. 13, 2018) (Haagen-Dazs sent thousands of text messages, claimed texts sent were not telemarketing).

11. Bowman v. Art Van Furniture, Inc., 2018 WL 6444514 (E.D. Mich, Dec. 10, 2018) (Art Van Furniture made over one million telemarketing calls marketing its furniture).

12. Krakauer v. Dish Network, L.L.C, 2018 WL 6305785 (M.D.N.C. Dec. 3, 2018) (Dish Network claimed it had no vicarious liability for over 51,000 calls made to consumers by third party contractors).

13. Peralta v. Rack Room Shoes, Inc., 2018 WL 6331798 (E.D. La. Dec. 3, 2018) (Defendant sent thousands of text messages to consumers, and claimed texts were not sent with an ATDS).

14. Lee v. Branch Banking & Tr. Co., 2018 WL 5633995 (S.D. Fla. Oct. 31, 2018) (Defendant claimed it had no vicarious liability for thousands of calls made).

15. Mattson v. Quicken Loans, Inc., 2018 WL 52552288 (D. Or. Oct. 22, 2018) (Quicken Loans claimed that procedures regarding repeated calls were adequate).

16. Abramson v. Oasis Power L.L.C., 2018 WL 4101857 (W.D. Pa. July 31, 2018), *report and recommendation adopted by* 2019 WL 4095538 (W.D. Pa. Aug. 28, 2018) (Oasis Power claimed calls were not made with an ATDS and it had consent to contact consumers).

17. Somogyi v. Freedom Mortg. Corp., 2018 WL 3656158 (D.N.J. Aug. 2, 2018) (Defendant claimed hundreds of thousands telemarketing calls were not made with an ATDS because there was human intervention).

18. Coulter v. Ascent Mortgage Resource Group L.L.C., 2017 WL 2219040 (E.D. Cal. May 18, 2017) (Defendant claimed it the phone numbers contacted were not generated by ATDS equipment and the company had consent to contact consumers).

19. Youngman v. A&B Ins. & Fin. Inc., 2018 WL 1832992 (M.D. Fla. Mar. 22, 2018), *report and recommendation adopted by* 2018 WL 1806588 (M.D. Fla. Apr. 17, 2018) (Defendant placed calls to 330,511 unique telephone numbers).

20. Gould v. Farmers Ins. Exch., 288 F. Supp. 3d 963 (E.D. Mo. Jan. 19, 2018) (Defendant claimed there were insufficient facts to show that an ATDS was used, and that it had no vicarious or direct liability for the thousands of text message advertisements sent).

21. Braver v. Northstar Alarm Servs., L.L.C., 329 F.R.D. 320 (W.D. Okla. 2018) (Defendant claimed that millions of telemarketing calls were not made with a prerecorded voice, because the calls employed the Soundboard system, in which only snippets of a prerecorded voice were used, and that it did not have vicarious liability for thousands of calls made).

22. Glasser v. Hilton Grand Vacations Co., L.L.C., 341 F. Supp. 3d 1305 (M.D. Fla. 2018), *appeal to 11th Circuit pending* (Hilton claimed that calls made to potentially thousands of class members were not through an ATDS because of human intervention).

23. Sasin v. Enterprise Fin. Group, 2017 WL 10574367 (C.D. Cal. Nov. 21, 2017) (Defendant claimed calls were not made to residential numbers to thousands of class members).

24. Melito v. American Eagle Outfitters, Inc., 2017 WL 3995619 (S.D.N.Y. Sept. 11, 2017) (appeal filed 2d Cir. Oct. 10, 2017) (American Eagle claimed it was not liable for text messages sent by third party in mass marketing campaign).

25. Golan v. Veritas Entertainment, L.L.C., 2017 WL 2861671 (E.D. Mo. July 5, 2017) (Over three million calls made, defendant claimed it had no vicarious liability).

26. O'Shea v. American Solar Solution, Inc., 2017 WL 2779261 (S.D. Cal. June 27, 2017) (American Solar Solution contacted nearly 900,000 consumers).

27. Hooker v. Sirius XM Radio, Inc., 2017 WL 4484258 (E.D. Va. May 11, 2017) (One of at least four class actions challenging unwanted telemarketing calls; defendant moved to compel arbitration).

28. Liotta v. Wolford Boutiques, L.L.C., 2017 WL 1178083 (N.D. Ga. Mar. 30, 2017) (Defendant sent text messages to over 4,000 consumers).

29. Gibbs v. SolarCity Corp., 239 F. Supp. 3d 391 (D. Mass. Mar. 8, 2017) (SolarCity made telephone calls to thousands of consumers).

30. Hoover v. Sears Holding Corp., 2017 WL 639893 (D.N.J. Feb. 16, 2017) (Sears claimed it had consent to send text messages to thousands of consumers).

31. Meyer v. Bebe Stores, Inc., 2017 WL 558017 (N.D. Cal. Feb. 10, 2017) (Defendant claimed that there was no proof that ATDS was used, and claimed that it had consent to send text messages to 38,600 class members).

32. Mohamed v. American Motor Co., L.L.C., 320 F.R.D. 301 (S.D. Fla. 2017) (Defendant claimed it had no vicarious liability for the text messages sent to thousands of consumers).

33. Stevens-Bratton v. TruGreen, Inc., 675 Fed. Appx. 563 (6th Cir. 2017) (Defendant claimed that the system used to contact consumers was not an ATDS).

Mr. DOYLE. Thank you, Ms. Saunders.

Mr. Halley, you are now recognized for 5 minutes.

STATEMENT OF PATRICK HALLEY

Mr. HALLEY. Thank you. Chairman Doyle, Ranking Member Latta, members of the subcommittee, thank you for the opportunity to appear before you today. My name is Patrick Halley. I am a senior vice president of Regulatory Affairs and Advocacy at USTelecom–The Broadband Association.

Illegal robocalls are a major problem and it is timely and appropriate that this committee is laser-focused on potential solutions. USTelecom and our members share your commitment to doing everything we can to eliminate bad actors. Beyond the daily deluge of calls, consumer business and government agency numbers are being spoofed without their knowledge. And while I don't pretend to be as important as the Moffitt Cancer Center, in the last 3 weeks my number has been spoofed on multiple occasions resulting in calls and voice mails from angry people demanding that I stop calling them. Calls I never made, so I understand this on a personal level.

Along with our members, USTelecom is working daily to enhance our knowledge about the calls that traverse our networks in order to block illegal calls and provide consumers with better information. Our efforts are designed to empower consumers by providing more information about the identity of callers and enabling them to block the calls that they do not want to receive. Why do we do this? Because consumers demand it. Because it undoubtedly reduces the ability of fraudsters to achieve their objectives and because it increases the confidence of consumers and businesses that rely on our networks. The idea that people aren't answering phone calls is not good for anybody including our members and consumers and businesses.

In addition to improving the consumer experience, we are equally focused on facilitating coordination with Federal and State enforcement authorities including the FCC, the FTC, and State Attorneys General. By helping law enforcement agencies quickly identify the source of illegal callers, together we can bring criminals to justice. Those who blatantly disobey the law and who enable fraudulent activity need to go to jail.

As the subcommittee considers potential legislative solutions, I would like to highlight three areas where our members are taking the lead in addressing the scourge of illegal robocalls. First, industry has undertaken considerable efforts to deploy call authentication technologies, commonly referred to as STIR/SHAKEN, that will substantially diminish the ability of illegal robocallers to spoof caller ID information. Companies of all types and sizes are deploying these standards into their IP networks today and will continue to do so throughout 2019. Once deployed, consumers will have more information about caller identity and the types of calls that they are receiving and carriers will be able to more accurately identify the source of calls which will improve call traceback efforts. Testing of the new technology and products is well underway.

Second, more tools are available today than ever before for consumers to mitigate illegal or unwanted robocalls. A significant

number of voice providers are increasingly integrating these tools into their networks and hundreds of applications are available to consumers on their smartphone. Importantly, facilities-based providers are increasingly developing robocall mitigation tools themselves including directly into their networks. For example, AT&T's Call Protect Service automatically blocks suspected fraudulent calls, and Verizon provides a Spam Alert service for wire line customers and has also rolled out free spam alerting and call blocking tools to wireless customers.

Carriers including USTelecom members, CenturyLink, Windstream, Frontier, Consolidated, and others are also deploying a variety of additional tools across their TDM and IP networks, including anonymous call rejection and no solicitation services. Multiple providers also work with companies like Nomorobo with a one-click solution to facilitate their customers' ability to use third-party call blocking services.

Third, USTelecom's Industry Traceback Group is expanding its efforts to identify the source of illegal robocalls and working in close coordination with Federal and State agencies on enforcement efforts. There are currently 27 members of the Traceback Group including traditional wireline phone companies, wholesale carriers, wireless providers, and cable companies, so it is an industrywide effort. The members also include foreign carriers and non-traditional voice providers.

Recently, we significantly enhanced our ability to trace back calls by automating the process. The time it now takes to trace back an illegal robocall has been reduced from weeks to days, sometimes even hours. And while our members will continue being vigilant and proactive to combat illegal robocalls, we will need to continue our collaborative approach with our partners in government. We welcome the opportunity to work with Congress on additional ways we can stop these illegal scammers at the source and bring them to justice. Thank you and I look forward to answering your questions.

[The prepared statement of Mr. Halley follows:]

Written Testimony of Patrick Halley
Senior Vice President, Advocacy and Regulatory Affairs
USTelecom – The Broadband Association

"Legislating to Stop the Onslaught of Annoying Robocalls"

April 30, 2019

Chairman Doyle, Ranking Member Latta, Members of the Subcommittee, thank you for giving me the opportunity to appear before you today. My name is Patrick Halley, and I am Senior Vice President of Advocacy and Regulatory Affairs at USTelecom – The Broadband Association.

USTelecom is the nation's trade association representing broadband providers, suppliers, and innovators connecting our families, communities and enterprises to the future. Our diverse membership ranges from large publicly traded global communications providers, manufacturers, and technology enterprises, to small companies and cooperatives – all providing advanced communications services in urban and rural markets, and everything in between.

USTelecom and our members share this Subcommittee's desire to eliminate the plague of illegal and unwanted robocalls and we appreciate your focus on potential solutions to address the problem. Along with our members, we are working daily to enhance our knowledge about the calls that traverse our networks in order to block illegal calls and provide consumers with more information about the calls they receive. Our efforts are designed to empower consumers by providing more information about the identity of callers and enabling them to block calls they do not wish to receive. We do this because our customers demand it, because it undoubtedly reduces the ability of fraudsters to achieve their objectives, and because it increases the confidence of consumers and businesses that rely on our networks. As the FCC recently stated, "it is obvious that the volume of unwanted calls is reducing the value of telephony to anyone who makes or receives calls."[1] This is a problem the industry is committed to solving.

In addition to improving the consumer experience, we are equally focused on facilitating enhanced coordination with federal and state enforcement authorities, including the Federal Communications Commission (FCC), the Federal Trade Commission (FTC) and state Attorneys General. By helping law enforcement agencies quickly identify the source of illegal callers, together we can bring criminals to justice. The ongoing civil enforcement efforts of the FCC and the FTC are critical. However, increased criminal enforcement against illegal robocallers is necessary.

As the Subcommittee considers potential legislative actions to address the robocall plague, I would like to highlight three areas of active industry leadership to address the problem.

---

[1] *See Advanced Methods to Target and Eliminate Unlawful Robocalls*, Second Report and Order, FCC 18-177, CG Docket No. 17-59 at para. 4 (Dec. 2018) (describing the "multi-prong approach" to address the problem of unwanted calls).

- First, industry has undertaken considerable efforts to deploy call authentication technologies, commonly referred to as STIR/SHAKEN, that will substantially diminish the ability of illegal robocallers to spoof caller-ID information. Companies of all types and sizes are deploying these standards into their IP networks today and will continue to do so throughout 2019. Once deployed, consumers will have more information about the identity of a caller or the type of call they are receiving. And carriers will be able to more accurately identify the source of calls, which will improve call traceback efforts.

- Second, more tools are available today than ever before for consumers to mitigate illegal or unwanted robocalls. A significant number of voice providers are increasingly integrating these tools into their networks and hundreds of applications are available to consumers on their smartphones.

- Third, USTelecom's Industry Traceback Group ("Traceback Group") is expanding its efforts to identify the source of illegal robocalls and working in close coordination with federal and state agencies to assist in enforcement efforts. Recently, we have significantly enhanced our ability to traceback calls by automating the process. The time it now takes to trace back illegal robocalls has been reduced from weeks to days – sometimes even hours.

Beyond simply implementing STIR/SHAKEN and participating in the Traceback Group, many carriers are taking steps to require others to do the same. Our members do not want to do business with other carriers that are not taking sufficient steps to address the problem. For example, some carriers are amending their contracts so that the entire call path for calls received from upstream carriers is with companies that are participating in traceback efforts. In addition, carriers are actively monitoring traffic over their networks to ensure their customers are not making illegal calls, and to identify other providers that appear to be carrying illegal traffic – and then taking steps to help those other carriers fix the problem or to no longer do business with them.

As the FCC's Chief Technology Officer and Enforcement Bureau Chief noted in recent letters to providers encouraging participation in the USTelecom Industry Traceback Group, "neither government, nor industry, without the active assistance of the other, can hope to stem the flood of scam calls plaguing consumers across the country."[2] USTeleeom greatly appreciates the collaborative work we do with our partners in government and we welcome the opportunity to work with Congress on additional steps that can be taken.

Industry is Committed to the Deployment of Call Authentication Standards.

Industry is swiftly moving to implement the STIR/SHAKEN call authentication standard. Once implemented, the ability of illegal robocallers to spoof caller-ID information will be significantly reduced and consumer knowledge about the validity of incoming calls will substantially increase. Last year, the industry-led Governance Authority for the SHAKEN standard was established under The Alliance for Telecommunications Industry Solutions (ATIS), the standards body coordinating industry implementation of the SHAKEN protocol. And next

[2] Press Release, FCC, FCC Calls on Network Voice Providers to Join Effort to Combat Illegal Spoofed Scam Robocalls (Nov. 6, 2018), https://docs.fcc.gov/public/attachments/DOC-354942A1.pdf.

month, ATIS is expected to identify the Policy Administrator that will oversee the day-to-day operations of the SHAKEN standard.

Numerous voice providers – representing the wireline, wireless, and cable industries – have committed to deploying the SHAKEN and STIR standards within their respective networks.[3] While deployment depends on the timely and practical availability of vendor network upgrades and applications and there are some differences in the specific timelines to deployment of the SHAKEN and STIR standards, implementation efforts started in 2018, with most targeting deployments in their IP networks as soon as the end of 2019. Testing of the new technology and products is well under way. In March, AT&T and Comcast successfully verified authentication of calls between their separate networks, and Verizon announced the first exchange of STIR/SHAKEN-enabled calls to and from wireless customers.

While deployment of the SHAKEN and STIR standards is not a panacea to the robocall problem, these standards will improve the reliability of the nation's communications system by better identifying legitimate traffic. The deployment of the SHAKEN standard will also facilitate the ability of stakeholders (such as USTelecom's Traceback Group) to identify illegal robocalls and the sources of untrustworthy communications.

Robocall Mitigation Tools are Increasingly Available to Consumers Across a Variety of Voice Platforms.

Voice providers themselves and independent application developers are increasingly offering services that can help Americans reduce unknown and potentially fraudulent calls. Like efforts to authenticate calls, these tools alone will not solve the robocall problem, but they are an important tool that empowers consumers with the ability to better identify and/or block illegal or unwanted robocalls.

Importantly, facilities-based providers are increasingly developing robocall mitigation tools themselves, including within their networks. For example, AT&T's "Call Protect" service for customers with IP wireline phones, iPhones and HD Voice enabled Android handsets automatically blocks suspected fraudulent calls.[4] When activated, AT&T will automatically block fraudulent calls, warn of suspected spam calls, and allow consumers to block unwanted calls from a specific number.

In addition, through its Spam Alerts service, for all wireline customers who have Caller ID (including ones served on legacy copper technology), Verizon provides enhanced warnings about calls that meet Verizon's spam criteria by showing the term "SPAM?" before a caller's name on the Caller ID display. Using TNS's Call Guardian and Neustar's Robocall Mitigation solution, the Spam Alerts feature proactively identifies and warns customers about potentially malicious robocalls. Verizon has also rolled out free spam alerting and call blocking tools to wireless customers whose smartphones support these features. Consumers can better decide if they want to answer a particular call, or they can choose to have spam calls sent straight to

---

[3] *See e.g.*, FCC, Combating Spoofed Robocalls with Caller ID Authentication, https://www.fcc.gov/call-authentication (last visited Apr. 28, 2019).
[4] *See* AT&T, AT&T Mobile Security & Call Protect, https://www.att.com/features/security-apps.html (last visited Apr. 28, 2019).

voicemail.

Carriers, including USTelecom members CenturyLink, Windstream, Frontier, Consolidated and others, are also deploying a variety of additional tools across their TDM and IP networks, including "anonymous call rejection" services that block callers who intentionally mask their phone numbers and "no solicitation" services that make unidentified callers go through a screening step before ringing. Multiple service providers also work with Nomorobo to facilitate their customers' ability to use that third-party blocking service. Additionally, Metaswitch provides a robocall blocking service that supports all voice infrastructure and switches, from legacy Class 5 TDM to Metaswitch's pure VoIP systems.[5]

There are also numerous third-party scoring and labelling analytics tools for wireless consumers. In 2016, there were approximately 85 call-blocking applications available across all platforms. By October 2018, there were over 550 applications available, a 495% increase in call blocking, labeling, and identifying applications to fight malicious robocalls. The multitude and diversity of tools across multiple platforms is a testament to industry's commitment to empower consumers, regardless of the type of network involved.

Industry Traceback Efforts are Critical to Identifying the Sonrce of Illegal Robocalls.

Equally important for reducing illegal robocalls is the ability to identify the source of calls and a strong partnership between industry and government to share such information to go after bad actors. USTelecom leads the Industry Traceback Group whose members are committed to identifying the source of illegal robocalls, and working with law enforcement to bring these illegal actors to justice. The FCC's 2017 Strike Force Report contains a detailed overview of the Traceback Group.[6]

There are currently 27 members of the Traceback Group, including traditional wireline phone companies, wholesale carriers, wireless providers, and cable companies. The membership also includes foreign carriers (*e.g.*, Bell Canada), and non-traditional voice providers (*e.g.*, Google and YMax).[7] The Communications Act permits voice providers to share customer proprietary network information (CPNI) in order to protect their customers and/or networks, enabling USTelecom's Traceback Group to quickly and efficiently identify the path of calls under investigation.[8]

Since late 2017, USTelecom has been making enforcement referrals to the FCC and the FTC based on the traceback results of the group. This industry/government partnership helps to

---

[5] *See* Metaswitch, Robocall Blocking Service, https://www.metaswitch.com/solutions/fixed-line-solutions/robocall-blocking-service) (last visited April 28, 2019).

[6] *See* Letter from Brian Scarpelli, Senior Policy Counsel, ACT – The App Association; Thomas E. Goode, General Counsel, ATIS; Krista Witanowski, Ass't Vice President, Regulatory Affairs, CTIA; and Kevin G. Rupy, Vice President, Law & Policy, USTelecom, to Marlene H. Dortch, Secretary, FCC, CG Docket No. 17-59 at 19 – 23 (filed Apr. 28, 2017), available at: https://ecfsapi.fcc.gov/file/10428413802365/Ex%20Parte-Strike-Force-Report-2017-04-28-FINAL.pdf.

[7] *See* Appendix for list of Industry Traceback Group participating companies.

[8] Section 222(d)(2) of the Communications Act permits telecommunications carriers to share, disclose and/or permit access to, CPNI in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." 47 U.S.C. § 222(d)(2).

streamline the enforcement efforts of both the FCC and the FTC who can now avoid the time-consuming process of issuing subpoenas to every provider in the call path. Instead, they can more efficiently focus their efforts only on those upstream providers that have declined to cooperate with the efforts of the Traceback Group. Late last year, the FCC acknowledged that USTelecom's manual traceback process had reduced the time necessary for the agency to conduct its own traceback investigations from "months to weeks" and called the Traceback Group's work "instrumental" in helping the Commission to achieve its goal of taking swift action against illegal robocallers.[9] Recently, USTelecom modified its previous manual traceback process to one that is largely automated. The automated process will enable a significantly greater number of tracebacks and dramatically reduces the amount of time for each traceback. These efficiencies will better assist investigations by the FCC and the FTC.

While numerous providers have joined USTelecom's Traceback Group, and many others cooperate in good faith, several upstream carriers refuse to cooperate. This not only prevents the Traceback Group from identifying the true origin of some calls, but it makes subsequent law enforcement investigations more time consuming. Given the crucial role of traceback in mitigating illegal robocalls, Congress and federal enforcement agencies should strongly encourage voice providers to participate in traceback efforts. To that end, while we are still assessing its potential impact, we appreciate the objectives of Rep. Latta's discussion draft "STOP Robocalls Act" that, in part, seeks to ensure call information from interconnected VoIP, including one-way VoIP services, is available for tracebacks.

More Criminal Enforcement of Illegal Robocallers is Necessary.

Ongoing federal civil enforcement efforts are essential. For example, the FCC last year approved a $120 million fine against one illegal robocaller responsible for generating billions of calls. The FTC recently issue fines ranging from $500,000 to $3.6 million and shut down four separate operations responsible for bombarding consumers nationwide with billions of unwanted and illegal robocalls pitching auto warranties, debt-relief services, home security systems, fake charities, and Google search results.[10]

These civil enforcement efforts are critical, and we support the objectives of Chairman Pallone's "Stopping Bad Robocalls Act" to allow the FCC to go after first time offenders and to increase the statute of limitations for such enforcement efforts. However, there is an acute need for aggressive criminal enforcement against illegal robocallers at the federal and state level. Criminal organizations and individuals engaged in illegal robocalling activity should be identified, targeted and brought to justice through criminal enforcement efforts. We applaud the proposed legislation by members of this subcommittee seeking to increase forfeiture penalties. However, fines alone are insufficient. Of particular note in the FTC's recent announcement is the acknowledgement that two of the individuals named in the complaint are "recidivist robocallers," who were each targeted in earlier FTC lawsuits brought in 2017 and 2018. Beyond

[9] *See* Letter from Rosemary Harold, Chief, Enforcement Bureau, FCC, and Eric Burger, Chief Technology Officer, FCC, to Jonathan Spalter, President and CEO, USTelecom at 1 (Nov. 6, 2018), available at: https://docs.fcc.gov/public/attachments/DOC-354942A2.pdf.

[10] *See* Press Release, FTC, FTC Crackdown Stops Operations Responsible for Billions of Illegal Robocalls, (rel. March 26, 2019) https://www.ftc.gov/news-events/press-releases/2019/03/ftc-crackdown-stops-operations-responsible-billions-illegal.

these civil penalties, those who blatantly disobey the law and who enable fraudulent activity need to go to jail USTelecom and its industry partners stand ready to assist the government in bringing these bad actors to justice Indeed, the ultimate goal of USTelecom's Traceback Group is to identify the source of the worst of these illegal calls, and enable further enforcement actions by federal agencies

U S Attorneys' offices across the country should prioritize enforcement where federal statutes, such as the Truth in Caller ID Act, are implicated, and should work closely with the FCC and FTC and international partners in enforcement cases, particularly when the calls originate outside of the United States Another possible vehicle could be the Task Force on Market Integrity and Consumer Fraud, comprised of a number of divisions of the Department of Justice (DOJ), including the FBI and various United States Attorney's Offices as designated by the Attorney General [11] The focus of the Task Force is to investigate and prosecute consumer and corporate fraud that targets the public and the government, with a particular emphasis on the elderly, service members and veterans Given its focus on fraud directed towards consumers, as well as the inclusion of criminal enforcement agencies, the Task Force could be an ideal vehicle for pursuing criminal enforcement against illegal robocallers The Spam Calls Task Force Act of 2019's proposed establishment of an interagency working group under the Attorney General, would also further enhance federal and state criminal law enforcement efforts against illegal robocallers

There is no single solution to ending the scourge of robocalls, but progress is being made every day USTelecom and our members – along with our wireless and cable partners – are strongly committed to working together with government to substantially reduce, and ultimately eliminate this problem

[11] *See* Exec Order No 13844, 83 Fed Reg 33115 (July 11, 2018) available at https //www whitehouse gov/presidential-actions/executive-order-regarding-establishment-task-force-market-integrity-consumer-fraud/

Appendix: USTelecom Industry Traceback Participants

- Alliance
- ANI Networks
- AT&T
- Bandwidth
- Bell Canada
- Brightlink
- CenturyLink
- Charter
- Cincinnati Bell
- Comcast
- Consolidated
- Cox
- Frontier
- Google
- IDT Telecom
- Impact Telecom
- Inteliquent
- NovaTel
- O1 Communications
- Peeress
- Silver Star
- Sprint
- T-Mobile
- Verizon
- West Telecom
- Windstream
- YMax

Mr. DOYLE. Thank you very much. Thank you, Mr. Halley.

Mr. Foss, you are now recognized for 5 minutes.

STATEMENT OF AARON FOSS

Mr. FOSS. Chairman Doyle, Ranking Member Latta, members of the committee, thank you for giving me the opportunity to appear before you today. My name is Aaron Foss and I am the founder of Nomorobo.

Six years ago, my idea for stopping robocalls was chosen as the winner of the FTC's Robocall Challenge and since then we have stopped over 1 billion robocalls from reaching Americans, and that is billion with a B. We have prevented hundreds of millions of dollars from being stolen from Americans and I can only imagine how many life savings are still intact thanks to Nomorobo.

And as proud as I am of that number, I know it is just a drop in the bucket in solving this enormous problem. Billions of illegal robocalls are made every month, and there seems to be no end in sight. Mr. Latta mentioned that the FTC received 3.8 million complaints every year. We stop that many robocalls every day and a half, right, and on a best guess we are protecting less than one percent of all phone lines in the United States.

I am going to keep my remarks brief because I would really like to get down to the important task at hand which is having a meaningful conversation about stopping the robocall epidemic.

So, I just want to start by stepping back in time and looking at how far we have come. When I first started Nomorobo, the industry said it wouldn't work. We would block too many good calls; the scammers would change tactics. Back then, the carriers weren't even sure that they could block robocalls due to FCC regulations. But we proved that robocall blocking does indeed work and today we are protecting millions of people each and every day from getting scammed and annoyed by robocalls.

It is well understood now that a phone number reputation system is vital to stopping the robocall problem and yet robocalls are still at unprecedented levels. More still needs to be done. On April 15th, this year, Tax Day, we decided to change the game again, so we released a full, a real-time feed of all of the active IRS callback scammers, for free, to the carriers. We are publicly showing the scammers' phone numbers along with the recordings and transcriptions of the message that they are currently pushing out right now.

We are encouraging all companies to use this data to put an end to one of the longest-running and most notorious robocall scams of all time. If the industry uses this data, in theory we can eliminate the IRS callback scams right now. And to launch it, we took out a full-page ad in the New York Times. What better way to tell the world about a new product. We agonized over every word in this ad, but specifically the headline, right, "We can win the war against robocalls," and the "we" refers to all of us in this room today, phone companies, robocall blocking companies, lawmakers, regulators. If we work together it can be done.

So, I am going to end with a rather radical suggestion for every lawmaker in this room. Every day I am asked, right, what kind of laws can be made? Do we need more of them? What should we do?

So, I would just like to propose that we change the laws around sales robocalls from an opt-out system into an opt-in. Right now, you have to take action if you don't want to get the calls. But I believe that you should actually have to take action if you do want to receive them from certain parties, with the obvious exceptions.

In order to make sales robocalls you must have the current owners' express written permission. It doesn't matter if the call is being made to a mobile or a landline, a residential or a business one. It doesn't matter if your number is on the Do Not Call Registry or not. I sometimes get robocalls on my Skype line, right, over-the-top services are now getting attacked by these robocall problems. If you don't have the consent, the answer is no. You can't legally call that person with a prerecorded message.

But, honestly, this isn't the big problem. It is not with the legal robocallers, it is with the criminals. Mr. Walden said that. These are criminals. Criminals don't obey the law. So, I thank you again for this opportunity to talk about this huge problem. I have a ton of experience in this area and use me as a resource today or tomorrow or next week. Ask me anything. I am in the trenches each and every day fighting this battle for all Americans. Thank you.

[The prepared statement of Mr. Foss follows:]

Chairman Doyle, Ranking Member Latta, and members of the Committee, thank you for giving me the opportunity to appear before you today.

My name is Aaron Foss, and I'm the founder of Nomorobo. Six years ago, my idea for stopping robocalls was chosen as the winner of the FTC's Robocall Challenge.

Since then, we've stopped over one billion robocalls from reaching Americans. That's a billion with a B. We've prevented hundreds of millions of dollars from being stolen from Americans. I can only imagine how many life savings are still intact thanks to Nomorobo.

And as proud as I am about that number, I know that's just a drop in the bucket in solving this enormous problem. Billions of illegal robocalls are made every month and there seems to be no end in sight.

I'm going to keep my remarks brief because I'd like to get down to the important task at hand – having a meaningful conversation about stopping the robocall epidemic.

Let's begin by stepping back in time and looking at how far we've come.

When I first started Nomorobo, the industry said it wouldn't work. We'd block too many good calls. The scammers would change tactics. Back then, the carriers weren't even sure they could block robocalls due to FCC regulations.

Well, we've proved that robocall blocking does indeed work.

Today, we're protecting millions of people each and every day from getting scammed and annoyed by robocalls. It's well understood now that a phone number reputation system is vital to stopping the robocall problem.

And yet, robocalls are still at unprecedented levels.

More still needs to be done.

On April 15 this year, Tax Day, we decided to change the game again.

We released a real-time feed of all of the active IRS call-back scammers, for free, to the carriers. We are publicly showing the scammers' phone numbers along with recordings and transcriptions of the messages that they're currently pushing out.

We're encouraging all companies to use this data to put an end to one of the longest running and most notorious robocall scams of all time. If the industry uses this data, in theory, we can eliminate the IRS call back scams right now.

And to launch it, we took out a full-page ad in the New York Times, that I've included. What better way to tell the world, right?

We agonized over every word in that ad but specifically, the headline – "We Can Win The War Against Robocalls." The "We" refers to all of us in this room today – phone companies, robocall blocking companies, call originators, lawmakers, and regulators.

If we work together, it can be done.

I'm going to end with a rather radical suggestion for every lawmaker in this room.

I propose that we change the laws around sales robocalls from an "opt-out" system into an "opt-in" one. Right now, you have to take action if you **don't** want to get the calls. I believe that you should have to take action if you **do** want to receive them from certain parties.

In order to make sales robocalls, you must have the current owner's express written permission.

It doesn't matter if the call is being made to a landline or a mobile phone, a residential line or business one.

It doesn't matter if your number is on the Do Not Call registry or not.

If you don't have consent, the answer is 'No'. You can't legally call that person with a prerecorded message.

I thank you again for this opportunity to talk about this huge problem. I have a ton of experience in this area. Use me as a resource today. Ask me anything.

I'm in the trenches each and every day fighting this battle for all Americans.

Thank you.

WE CAN WIN THE WAR AGAINST ROBOCALLS.

"Hello. This is Agent Bloom calling you from tax crime investigation unit of Internal Revenue Services. This is to inform you that IRS has issued an arrest warrant against you and within one hour you will get arrested from your house..."

Sound familiar? Every day, thousands of people are victimized by robocalls like this. Criminals used to rob people with guns. Now they use the phone.

They pretend to be technical support and fool you into paying thousands of dollars to "fix" your computer. They pretend to be the Chinese Consulate and threaten (in Mandarin, of course) to have you deported. They pretend that you've won a free cruise or an all-inclusive vacation when all you've really "won" is a smaller bank account.

We at Nomorobo know a lot about phone scams. We've stopped over 1 billion robocalls since winning the FTC's Robocall Challenge back in 2013.

And we're just as frustrated as you are that this problem isn't going away faster. We know that more can be done to protect Americans from illegal, unwanted robocalls.

With that in mind, we're very excited to unleash a new weapon in this fight.

Beginning today, we're making our real-time feed of IRS call-back scammers available for *free*. We're hoping that all phone companies will use this data to help end one of the most notorious and dangerous robocall scams of all time.

Robocalls continue to plague all of us for one very basic reason—they work. Scammers only need a few victims in order to be wildly profitable. But when fewer calls get through, the economics change and they'll be forced to stop.

One day, robocalls will be a thing of the past. But until then, protect yourself and those you love by installing our app on your mobile phone, enabling Nomorobo on your landline, or using a product from one of our partners.

We're confident that by working together, we can end this epidemic and ultimately win the war against robocalls.

Find out more at nomorobo.com/irs

Nomorobo™
Stop Robocalls Now.

WWW.NOMOROBO.COM

Mr. DOYLE. Thank you, Mr. Foss. During your testimony, Mr. Soto got a robocall, so there is no escaping it.

I will now recognize myself for 5 minutes for questions.

Mr. Summitt, let me start with you. In your testimony you talked about the very real risks that your organization faces on a regular basis from spoofed calls and how these calls are not only used to get members of your organization to pick up the phone, but also to give away sensitive information. And worse yet, the credibility of your organization is also being undermined by spoofers using your phone number and name to make unknowing call recipients do the same.

Do you feel like the members of your organization and the patients that you treat are losing faith in the integrity and effectiveness of our Nation's phone system?

Mr. SUMMITT. Yes, sir. I do. And the reason I say that is because if I am a consumer or I am a patient at Moffitt and I am receiving a phone call that is not Moffitt, I am losing faith and trust in the system. I am losing the potential faith in my provider that somehow data has been leaked or worse, and now I am picking up the phone and giving away additional information by thinking I am speaking to someone who I am legitimately doing work with. It is very much a serious problem.

Mr. DOYLE. Thank you.

Mr. Foss, do you think it would be helpful for consumers if the phone carriers offered services like yours in an opt-out basis?

Mr. FOSS. Absolutely, yes.

Mr. DOYLE. Yes. And so, the people understand that, you know, what kinds of consumers do you think would most benefit from the technology that you and others have created that wouldn't benefit from it if the service was only available in an opt-in basis?

Mr. FOSS. Sure. So to start this conversation, let's just look at the spectrum of robocalls, right. Here are the illegal scams, right, the fake IRS and the fake Social Security. We can all agree that those completely need to be eliminated from the network. On the other side, it is the good robocalls—the police, the fire, the schools—we can all agree that those need to be allowed through.

And if we just look at—and the middle part is that gray area, right. These are the debt collection calls. These are the telemarketers. Let's leave those out of this whole discussion. On this side of the obvious bad robocalls, they should never be allowed on the network. They should be kept off the network, ingress, egress, built in at the level.

We don't need to be telling people that this call is a spam-likely call. We just need to make sure that they never get through. That is even what we did with our new product to the carriers with the IRS calls. It is roughly about 50 numbers that are active every single day. Those numbers should be blocked from the network immediately. We are providing recordings, transcriptions, we have proof that that is it. Why that can't be provided on an opt-out basis, right, protect the network that way? If you actually want to get these calls, turn it off. I think that would be a great step forward.

Mr. DOYLE. Thank you.

Ms. Saunders, part of the narrative about robocalls that frustrates so many people is the notion that these calls are coming

from overseas and efforts to shut them down are like playing Whac-A-Mole. However, in your testimony, you say that a large proportion of these illegal robocalls consumers receive are ultimately from or on behalf of large, well-established American companies.

I think we all agree that fraudulent calls should be blocked, but I am curious why we receive so many illegal calls from established domestic companies and why those companies are not being held accountable under current law. Why is that?

Ms. SAUNDERS. So I appreciate the question. The issue I think nobody disagrees with what Mr. Foss says, and I just want to emphasize that the reason I am not emphasizing scam calls is because everyone else is. I am just trying to focus on the other calls.

What I tried to show in my testimony, exhaustively, through many, many cases, is the number of calls that are made by existing American companies. And they obviously are making money from making these calls. They are making money through telemarketing or debt collection and they are choosing to continue making the calls regardless of whether or not the law, they are violating the law, because they think they can either argue in court that the law does not apply to them or convince the FCC that the law should not be interpreted in a way that it applies.

According to the YouMail statistics, which I quote on Footnote 7, only 47 percent of the robocalls currently made are scams. The rest are robocalls, some proportion of those are the wanted robocalls, which we all agree. But there is a lot of—there are 20, 30, 40 percent of calls that are unwanted that still need to be addressed and need to be addressed through the Telephone Consumer Protection Act.

Mr. DOYLE. You think Chairman Pallone's Stopping Bad Robocalls Act would reduce the number of those calls?

Ms. SAUNDERS. Yes, sir.

Mr. DOYLE. Thank you.

Mr. Halley, I just have a couple seconds. I understand you are a Caps fan. I was wondering if you were at the game last Wednesday.

Mr. HALLEY. I was and so were some of your staff.

Mr. DOYLE. How did that game—see, at least in Pittsburgh when we get eliminated in the first round we just lose the first four games and it is not as painful as when the Caps take you seven games and then lose in double overtime. Yes, I just thought I would bring that up.

Mr. HALLEY. I don't want to get into a debate with you about the Caps or the Penguins, so let's leave that alone.

Mr. DOYLE. OK. I will yield back my time.

Now I yield 5 minutes to our ranking member, Mr. Latta, for 5 minutes.

Mr. LATTA. Well, again, thanks very much, Mr. Chairman, for holding today's hearing. Thanks again to our witnesses for being here.

Mr. Halley, if I could start my questions with you, can carriers currently offer their consumers tools to block robocalls?

Mr. HALLEY. They can and they do.

Mr. LATTA. OK, thank you. And how are those tools offered to consumers?

Mr. HALLEY. Sure. You know, some of them are sort of, for example, with Nomorobo a lot of our companies have initiated a capability where a customer can just online click a button and it essentially activates the Nomorobo service. Some of them are building those solutions directly into the network, but, you know, through traditional marketing information they make that information available to companies. USTelecom also makes information available on our website about different solutions.

Mr. LATTA. Do consumers take the additional effort to opt-in to these services and, if so, what is the adoption rate of those services?

Mr. HALLEY. So they definitely do. I cannot give you a specific answer in terms of the actual adoption rate other than I can tell you given the distaste and concerns that consumers have they are increasingly adopting those services.

Mr. LATTA. And the bill that we have introduced in the STOP Robocalls Act carriers would have the ability to provide call blocking technology as the default standard. Would this help in our fight against the bad actors out there?

Mr. HALLEY. So I think the ability for carriers to sort of on a default basis be able to block certain calls would have a positive effect. At the same time, I think there are some concerns about liability. This is a highly litigious area, obviously, and sort of the concerns about blocking certain calls on an opt-out basis could be an issue.

So I think if we were going to do that it would be helpful if there was sort of a safe harbor that says, you know, if you are blocking calls because they are not authenticated or if you are blocking calls because they are known to be fraudulent because of certain best practices or lists, et cetera, then, sure, as long as there is a safe harbor I think that would be a good thing.

Mr. LATTA. Thank you.

Mr. Chairman, I would like to ask for unanimous consent to enter into the record letters from CTIA and the American Cable Association for supporting this opt-out approach in the STOP Robocalls Act.

Mr. DOYLE. Without objection, so ordered.

[The information appears at the conclusion of the hearing.]

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

Mr. Summitt, in your testimony you mentioned that bad actors have fraudulently used healthcare organizations' names when making illegal robocalls and have even spoofed the phone numbers of these organizations to scam victims out of their personal information. I have heard of instances where private entities who experienced similar situations have shared information with Federal authorities to be helpful in investigating and stopping bad actors. The STOP Robocalls Act would help streamline this process so there is an easy way for entities whose names and numbers are being spoofed can alert the correct authorities.

Do you think a process that is described in our bill would be beneficial in protecting consumers and patients?

Mr. SUMMITT. Absolutely. I am in full agreement of that and, in fact, there is a whole movement in our cyber area as well across the Nation in collaborative work in sharing data with different places. This falls under that very same concept and it works. And if we had a method to where we could immediately call someone within the telecom community to help us put down some of these calls that would be one of the best things that we could possibly do. At present, I can give you an example and have in my testimony where we have tried to call our carrier and we do not get assistance.

Mr. LATTA. OK, thank you.

Mr. Halley, industry has already done a lot in this space outside of STIR/SHAKEN and the traceback initiative. Would this help existing efforts in rooting out the bad actors?

Mr. HALLEY. Absolutely. The more information we have about the identity and how to contact different carriers to make sure that we can effectively trace back calls and get to the source of the calls would be helpful.

Mr. LATTA. OK, let me follow up. On the traceback, Mr. Halley, on this initiative I just mentioned, I understand that USTelecom manages the traceback process. Can you briefly describe that process?

Mr. HALLEY. Sure, I would be happy to. So I think one thing that is important to understand is, you know, if I am a, you know, I have an AT&T subscriber in Silver Spring, Maryland and I am going to call my mom who is a Spectrum subscriber in Port Orange, Florida, it is not the case that a call just goes from one carrier and—boom—it just ends up with the other carrier, right. There are often multiple carriers, transit companies involved.

So, I will initiate a call which will be handed off to one carrier who will then hand it off to another carrier and then it will ultimately arrive at the final destination. So, the traceback process is all about figuring out who the source of the call was. And the way we do that is we identify, OK, this number was dialed, this was terminated at this number. Who did the call come from upstream? And once we identify that person, we then identify who did the call come from prior to that upstream, all the way back to the source of the original call.

And so, what we are able to do is determine, based on who was called and the number that they were called at, who was the actual carrier that originated that call and therefore who was the source of that call. And that is extremely helpful and we work every day with the FTC and the FCC and States to help them with information about who are enabling these calls from a carrier side and from the actual source.

Mr. LATTA. Well, thank you very much.

Mr. Chairman, my time has expired and I yield back.

Mr. DOYLE. The gentleman yields back. The Chair now recognizes Mr. McNerney for 5 minutes.

Mr. MCNERNEY. I thank the chairman for holding this hearing and I thank the witnesses this morning. Your testimony is very, very good and very informative.

Mr. Summitt, despite the growing attention on the annoying and abusive problem of robocalls, the number is actually increasing. We

have been hearing that. I am hearing it from my constituents. As we move forward with these bills, it is important to understand what is driving this increase. Would you say that the increase in fraudulent robotics, robocalls is due to the success in these calls in scamming money and getting more money? Do you think that is why we are seeing the increase or that is part of it?

Mr. SUMMITT. The tactics are getting more sophisticated. If I can reach the masses with legitimacy, I am going to have a better result. And I can tell you, I entered the healthcare field from a Defense Department career after 21 years and I have been in the healthcare field for 8 years. When I entered that I was actually manager of a telecom of another hospital system. I did not see this problem 8 years ago. If it was there, it was very low. Now we are in a time where it is so bad that we are impacting patient care.

Mr. MCNERNEY. It must be that these folks are making money doing it.

Mr. SUMMITT. They are making money and they are doing it on the backs of our patients and other consumers and in that process they are hurting us very, very badly.

Permit me for a moment, but one of the things that I am hearing here, we have capabilities today. Our technology today can do things to help put this down and I am asking for that to be pushed forward faster than what it is. When Mr. Halley's describing going from carrier to carrier to carrier and you have the traceback function, there is already the admission that we have the capability to know where these phone calls come from. It can be done. Why are we not pushing this forward at every phone call and making that part of the protocol of the communications that go from carrier to carrier to carrier?

And when I receive that on the end and I am getting a phone call from the U.S. Department of Justice, why am I not expecting for that phone call to be actually from the U.S. Department of Justice?

Mr. MCNERNEY. OK, thank you.

Mr. Halley, following up on the chairman's comments on the threat that these phone calls are making our phone system obsolete, do you expect to see technological strides in curbing unwanted phone calls coming in time to prevent the loss of faith in our Nation's phone system?

Mr. HALLEY. I do. I think we are doing everything we possibly can as an industry in close collaboration with government to address this problem. As has been stated, there is no—by the chairman—there is no silver bullet. This is going to require a combination of efforts from call-blocking services to traceback efforts and to, you know, authentication of the calls so that we know when a call is being made it is a real number not a spoof number.

And if we can do that, we can, you know, we can address the fact and figure out how to deal with calls that are being spoofed, including blocking them. So, there are a lot of things that are being done that will do this in a timely manner.

Mr. MCNERNEY. So with the STIR/SHAKEN technology that should allow consumers to see the ID of the phone call that is coming in, how much does a consumer need to get involved to protect themselves using that technology?

Mr. HALLEY. So it should be transparent to the consumers. This is just a very technological protocol that is sort of in the background. And what it will do, just to be clear, is it will provide information about the authenticity of the call in the sense that the call is a real number that has been dialed and it has been verified. It is not a number that has been spoofed.

It doesn't in and of itself block the call, right. It is just providing more information. It is providing the carriers more information so that they can determine, you know, what policies they are going to adopt with respect to calls that are not authenticated and it is going to provide more information to third-party analytics providers and ultimately to consumers so they can know——

Mr. MCNERNEY. The consumer is going to need to know what is going on so they can decide which phone calls to answer.

Mr. HALLEY. Absolutely. And there is going to be a consumer information component to all that too as to what it means when they are getting different information about what kind of a call it is.

Mr. MCNERNEY. Mr. Foss, do you believe that the Government and innovators have the tools to keep ahead of this arms race?

Mr. FOSS. That is a good question, right? Like technology always outpaces legislation and regulation, right, it has to, so these criminals are always going to be one step ahead. Our system is very adaptive, right, again we just saw the rise in neighbor spoofing a couple of years ago. When we first started out it was purely a blacklist system. Blacklisting doesn't work against the neighbor spoofing, right, those calls that look like they are coming from your area code and exchange.

So, I think that third-party providers like us, the carriers, all the organizations, if we had the framework to be able to do pieces of that then we can stay ahead of the changes, because I can guarantee, right, the only constant is change itself. The only thing I can guarantee about robocallers is that they won't stop, right. They will just keep on changing their tactics until they get through no matter what anybody does.

Mr. MCNERNEY. OK, thank you, Mr. Chairman.

Mr. DOYLE. The gentleman yields back. The Chair now recognizes Mr. Johnson for 5 minutes.

Mr. JOHNSON. Thank you, Mr. Chairman. I appreciate you having this hearing today. It is a very important subject.

Mr. Halley, do I have that right? Halley, is that the right pronunciation?

Mr. HALLEY. Halley, like Valley with an H.

Mr. JOHNSON. Halley, OK. You know, unwanted calls are not the only type of unwanted communications that people receive. I am sure every one of us in this room receives hundreds of thousands of emails per year that are unwanted and some might even be from scammers and fraudsters. What makes the phone system different and makes people more vulnerable to falling victim to these scams?

Mr. HALLEY. I think there is, you know, first of all, it is real time, right, so you don't have the opportunity to just, you know, decide whether or not you are going to ignore it, which is fairly easy in an email. And it is also just a highly personal communication, right, when somebody is calling sometimes with information about you specifically designed to trick you into doing something, right.

And so, there is just a certain element of the types of communications you get on a phone that are just fundamentally different than over via email.

Mr. JOHNSON. OK. Continuing with you, Mr. Halley, I think we can all agree that we want to go after bad actors and ensure that legitimate business communications can continue while the FCC and industry considers how to implement STIR/SHAKEN and call blocking and labeling technologies.

Do you see any value for consumers in having the ability to receive information about their healthcare, updates about their financial situation, or things like school closings that could potentially be mislabeled or blocked if analytics don't work properly for call blocking and labeling technologies?

Mr. HALLEY. Yes. I think it is important that all the work we do here, while we are getting smarter and smarter about the types of calls that are going over our networks and the analytics providers get better and better every single day, we do have to be careful not to block legitimate calls for certain.

Mr. JOHNSON. OK. Are there steps carriers are taking to ensure that calls are not mislabeled or improperly blocked?

Mr. HALLEY. Absolutely, on a daily basis. I can tell you that Mr. Foss' companies and others in the space, the analytics companies, work regularly to determine how to ensure that we are blocking the calls that should be blocked, but not blocking the calls that should get through.

Mr. JOHNSON. OK. What is the current process for unblocking or fixing mislabeled calls?

Mr. HALLEY. Sure. All the members that we work with have a process in place where a legitimate business can contact them to, you know, essentially protest the fact that a call is being blocked and try to make sure that the numbers that are being blocked are unblocked. I will say it is a subjective process, right. I think we need to be careful because we absolutely don't want to block calls that are legitimate and that might be from a school or a bank alerting me to a fraud or anything else that is positive. Just because somebody comes to a carrier and says, "Hey, that was a legitimate call, unblock me," we have to be careful, right. And so, we have a process in place to figure out how to handle that.

Mr. JOHNSON. I can tell you, you know, from a personal note, even something as simple as a potential scam or fraud alert on a call is very, very helpful to me. I mean I am not going to call out my carrier in a public hearing like this, but I can tell you that I have probably over the last 3 months begun to get alerts on certain phone numbers from my carrier saying, "Hey, we think this is a scam or a fraud alert." And I can ignore that call and, you know, throw it aside. I don't worry about it.

So, I can tell you that that is at a minimum is helpful to me. Continuing on, Mr. Halley, how does call blocking and labeling from carriers, such as many of your members, differ from call blocking and labeling from third-party app providers like that of Mr. Foss' company, Nomorobo?

Mr. HALLEY. Sure. So I think ultimately the technology behind call blocking and call labeling is similar whether it is something that is being done in a carrier network and, in fact, our carriers

are working with third-party analytics companies to build these capabilities directly into our networks. I don't think there is technologically a difference, it is just a question of how it is being implemented.

I don't know if you want to——

Mr. FOSS. Yes, if I could chime in. Yes, absolutely. Nobody wants the good calls stopped, right, nobody. We all want the bad calls stopped to all those pieces working together, right. In theory, everybody should have the same data like, you know, 2 weeks, 3 weeks, everybody can go and look back and say that was a robocall. The thing that we think that is going to be the main thing is detecting those very, very quickly.

So, there is the question, right, if we had a kind of a head-to-head, right, who is detecting them quicker or who is more accurate and things like that again working together that is ultimately where this comes in.

Mr. JOHNSON. Well, as an IT guy, I can tell you I am extremely inquisitive about the technology that lets you identify what those potential robocalls are, but we can't get into it now because my time has expired.

Mr. Chairman, I yield back.

Mr. DOYLE. I thank the gentleman and he yields back. The Chair now recognizes Mr. Loebsack for 5 minutes.

Mr. LOEBSACK. Thank you, Mr. Chair. I do want to thank Chairman Doyle and Ranking Member Latta for convening this hearing today, and also want to thank all these great witnesses here. This is obviously a huge problem for our constituents.

Like one of our other Members, Mr. Walden, he mentioned he had 20 town halls. I have had 20 Coffees with your Congressman. I can't say that in every single one this has come up, but in most of them it has especially in a place like Iowa where we have an aging population. I am aging myself and so I get a disproportionate number of these damn calls as well.

And, you know, I have—I sit here and I think, well, I have a cell number that I didn't think anybody had. I am a Member of Congress. How did this happen? Well, they can get through to all of us. That is the thing. It is just quite amazing. And we have got to have this relief, there is no doubt about it, because I do hear about this all the time. And it is a bipartisan problem because every one of our constituents, you know, could potentially be faced with this problem going forward.

I am glad that we have got a lot of these bills that we are talking about today. And it does seem like there are some technological limitations to the scope of these bills, so I do want to raise the question of what to do for the folks who don't have the latest and greatest technology, whether that means cell phones and smartphones with screens or home phones with some form of digital output. It strikes me that the Americans who are likely to lack these new technologies are likely to be older and potentially more vulnerable to the very sorts of criminals who call with a bogus story about owing taxes to the IRS or claim of a loved one in jeopardy or whatever the case may be.

So, to that point I have a couple questions for everybody. I am not going to pick out anyone in particular, I will just let you folks

go at it. I do want to discuss the challenges and limitations for implementing STIR/SHAKEN to the widest possible consumer base. I understand that gateways might be helpful on older networks. How could the use of gateways help make sure that rural customers in particular get access to these new ways to stop robocalls?

And I will just open that up to the panel and let you folks jump in.

Mr. HALLEY. So I think it is one of the limitations on the STIR/SHAKEN framework is that as it is currently designed, the STIR/SHAKEN standard works for IP traffic. It doesn't work for the TDM, you know, traffic that is the older copper networks and so that could have an impact on folks who are more dependent on the traditional telephone, you know, copper line telephone service.

With that being said, that is the current limitation on the standard and it is also important—two of the things I mentioned in my testimony, you know, no solicitation services or anonymous call rejection services, those will work over anything whether it is a TDM network or an IP network. And so, services like that if the number, if somebody has purposely masked their caller ID the call doesn't get through. Or if somebody doesn't go through the process of there is a human element before somebody actually it rings, there is a step has to be taken that this is, in fact, a real call.

So, there are things that can still be done to address that kind of traffic even though the current STIR/SHAKEN standard wouldn't be effective.

Mr. LOEBSACK. Anyone else? Yes, go ahead, Mr. Summitt.

Mr. SUMMITT. Yes, implementing STIR/SHAKEN in our organization would require us to basically redo our front end of our telecommunications system because we are not up to speed with that new technology. And we have looked into it, but the point is we are just one organization across the Nation to get this implemented and for every dollar I spend in trying to protect our organization or redoing infrastructure is a dollar away from care and research.

Mr. LOEBSACK. Anybody else? Yes, go ahead.

Mr. FOSS. For our solution, right, we piggyback right now off of simultaneous ring. It is available in theory on TDM, on IP, on mobile, on landline, right. We like the idea of being completely backwards-compatible. In theory, instead of like a gateway we could somehow do the STIR/SHAKEN lookup on behalf of the technologies and the carriers that can't support that. How that would play out, not exactly sure.

But it is absolutely, I think, important to—everybody just looks at the latest and greatest. You know, you have the brand-new, you know, fancy cell phones, but there are still tons of landlines and those are sometimes even more vital than even the mobile lines.

Mr. LOEBSACK. That is right.

Ms. Saunders, do you have anything you want to say?

Ms. SAUNDERS. The only thing I would like to point out, if I might, is that STIR/SHAKEN is a critically needed technology but it will not take care of all the problems of identifying who the callers are. As was explained in an article in the New York Times just last week, callers also have the ability to buy hundreds of phone numbers that are essentially anonymous. And when one number is

caught by this technology, they just switch to another phone number.

Mr. LOEBSACK. And I see my time is up. I apologize I have to interrupt, but I don't want us ever to forget about rural folks and older folks. Thank you very much and I yield back. Thank you.

Mr. DOYLE. The gentleman yields back. The Chair now recognizes Mr. Kinzinger for 5 minutes.

Mr. KINZINGER. Well, thank you, Mr. Chairman. And thank you all for being here and hopefully this won't take the whole time.

Mr. Summitt, you mentioned cases of criminals disrupting hospital business operations and committing financial fraud including by robocallers using spoofed numbers identical to the hospitals in order to gain sensitive patient information, which is not only bad at face value but it erodes trust between patients and their healthcare providers. As you put it, these calls are identified as a reputable source such as law enforcement or a government entity which is what heightens the likelihood of success.

I don't mean to put you on the spot, but Mr. Engel and I this year introduced a bill on 9–1–1 swatting. It is the Anti-Swatting Act. You may know that swatting is a hoax on an emergency services dispatcher using a form of spoofing. These perpetrators will call police forces and in some cases a SWAT team to a target's home and there have been cases where there have been tragic loss of life. And I have actually been a victim of swatting myself, early on.

I want to keep the theme today of moving with narrow, effective legislation aimed at bad actors, but public safety testified last year in support of this legislation because it would clearly define perpetrators for the criminals that they are. Have you had a chance to review that legislation? It is fine if you have not, but, if so, would you have any issue with something like that moving along with some of the others here today?

Mr. SUMMITT. And I apologize, I have not reviewed that specific one.

Mr. KINZINGER. That is fine.

Mr. SUMMITT. I have read every one being presented to here and but I have not read that one, but I would be in support of something to do that. And the other thing I just want to quickly say about all this, it is—I am not necessarily saying that we need to dump all this back on the telecoms, but I am saying we have technologies today that can and why are we not putting into place giving the callee, the recipient, enough information to know whether I want to answer this phone call or not. Again, if I see that caller ID, fine. It is my choice whether to answer that call or not. But I need to know that is who the person is. By protecting—and the arguments have been there are some legitimate reasons why they shouldn't be known, fine, let's put those as anonymized or restricted and it still gives me the responsibility to say I am going to answer or not that call.

Mr. KINZINGER. Thank you. Mr. Halley, your written testimony states that fines are sufficient to curb the scourge or, I'm sorry, insufficient to curb the scourge of robocalls. Why do you think fines are not enough to curb these bad actors, and is it that fines could

be steeper but enforcement is difficult or what do you attribute that to?

Mr. HALLEY. Sure. I think what you have heard today is that there are sort of a range of different types of robocalls, right.

Mr. LONG. Pull your microphone closer.

Mr. HALLEY. Sure. I think what you have heard today is that there are range of different types or robocalls, some that are, you know, from businesses who are conducting business for legitimate reasons, and then you have a significant portion of which are just blatantly illegal, and then some cases blatantly trying to commit a fraud. As Mr. Foss said, they don't care what the law is. And we can talk all we want about how the TCPA should be interpreted, et cetera, but they are not going to pay attention. They are just going to dial millions and billions of robocalls.

And so, the point there is, you know, we can double or even triple the fine under the act for those types of calls. They don't care.

Mr. KINZINGER. Yes. You are never going to be able to track it down.

Mr. HALLEY. So, we have to take these people and figure out how to put them in jail rather than impose fines on them.

Mr. KINZINGER. OK, so when we are going after these actors I understand that the authorities they only have a statute of limitation of about a year, I guess, to actually bring charges. What are your thoughts, you kind of went into this, on how to increase that time of statute of limitations so the good guys can do all they can to go after these folks, and what are the benefits or risk of expanding any statute of limitations?

Mr. HALLEY. I think we are supportive of expanding. There are different bills that have different, whether it is 2, 3, or 4 years, et cetera, and some of the bills handle it differently. But as a general matter, we think that making sure the FCC, the FTC, State AGs, have sufficient amount of time to go back and take action against bad actors is important. And as technology is developing, and I completely agree with what you said that there are solutions and we are working every day to implement them, sometimes the actual legal process just takes a long time. And so I think we are in favor of enhancing the statute of limitations.

Mr. KINZINGER. Excellent. Thank you all for being here and I yield back, Mr. Chairman.

Mr. DOYLE. The gentleman yields back. The Chair now recognizes Mr. McEachin for 5 minutes.

Mr. MCEACHIN. Thank you, Mr. Chairman. I want to thank you and Chairman Pallone for convening today's hearing on this issue that is—that all of our constituents care deeply about.

Today, unwanted robocalls are not only ubiquitous and a nuisance, they can be predatory. While some actors rely on robocalls to provide important information about appointments, school closures, and other matters, spam and phishing calls remain a problem. And as we have already heard today, we have got steps that providers can take to mitigate these spam calls on their own. SHAKEN/STIR technology and other innovative products like Nomorobo that aim to verify and authenticate calls are offering a promising start.

As Mr. Loebsack identified, we have some concerns about rural areas. And I want to start off, I guess, by asking Mr. Halley—is it, did I say that right, "Hailey"?

Mr. HALLEY. Hailey, Halley, whatever you want is fine with me.

Mr. MCEACHIN. Well, how——

Mr. HALLEY. Valley with an H.

Mr. MCEACHIN. Well, how does your daddy pronounce it?

Mr. Halley, thank you, sir. Are there models in Europe that we could be looking at that would allow us to use technology like SHAKEN/STIR in rural areas that are copper-dependent, as you suggested that is a current limitation of the technology now. How do we expand it into rural areas? What can we do? It is my understanding there might be models in Europe that we could emulate.

Mr. HALLEY. So I don't know the answer to that question, unfortunately, but I would be happy to answer that after the hearing. I don't know if anyone else knows about European?

Mr. MCEACHIN. I was going to turn to Mr. Foss. I thought in sort of your piggyback on there that you suggested there are some ways that Nomorobo can be adapted to I think you said older technologies. You may not have said "older technologies" but that is what I heard. Is that correct?

Mr. FOSS. Yes, absolutely. And again, if we are at the network level, right, as Mr. Halley was saying is that each call is kind of passed throughout the different levels of the network, right. If we had something that was again a spam scam filtering at the network level, even higher up, right, those results would trickle down to all of the phones in the network whether it is rural, whether it is landline, whether it is mobile and absolutely protect those constituents.

Mr. MCEACHIN. Now what can we do here in the Congress to help provide an atmosphere to allow that type of technology to move forward? Because you look at my district, I represent the 4th district of Virginia and yes, we have good urban populations and centers, but we also have wide swathes of rural Virginia which we tend to call Southside Virginia.

How do we make, get that technology spread to Southside Virginia which is again mostly rural?

Mr. FOSS. Sure. So why don't I tell you about the difficulties that I have when we talk to some of the carriers, right, what are some of the objections, what are some of the things that they are concerned about. And again, Mr. Halley knows it, right. Number one is, are we only blocking the calls that should be blocked, right.

So again, if you were to use our entire database, right, the 1½ million numbers that we have there, are there a swath of robocallers in there that should or should not be blocked? It is up for debate, right, that we are an editorial service, our users say that we do not, you know, they do not want to get these calls, therefore they are hiring us, right.

If there were things like safe harbor, if there was more on the legal side, right, that is even with our IRS offering, we are making a transcription and a recording, you know, today what that number is, the message that is being pushed out, that should give the carriers enough confidence to be able to say, "Yes, we can shut this down at the network level." And again, Mr. Halley can probably

shed some light on that of if there was a safe harbor, if there was something where, you know, using a data provider like us or their own internal things and they go and do this that there wouldn't be the legal ramifications if something did go wrong.

Our false positive is, last month was 0.07 percent, right, less than a tenth of a percent. Our users know that it is very accurate. Our accuracy was over 97 percent, right, we only missed like 3 percent of those calls. But that would be what I would think if the carriers, whenever we go to a carrier and say, "Hey, go and integrate this," they are definitely worried what happens if we stop good calls. We know the answer that you are not going to, but I think that that would give the industry more impetus or more encouragement to use services like us.

Mr. MCEACHIN. I appreciate you and I appreciate you all being here today. Thank you, Mr. Chairman. I yield back.

Mr. DOYLE. The gentleman yields back. The Chair now recognizes Mr. Bilirakis for 5 minutes.

Mr. BILIRAKIS. Thank you. Thank you, Mr. Chairman. I really appreciate you holding this hearing.

This is something that is affecting all of us, but particularly our seniors what they are going through. Inexcusable what is happening, particularly, Mr. Summitt, your testimony with regard to Moffitt which is in my area. Sixty-six hundred calls in 90 days and that information, I mean and our patients, cancer patients, you know, they are being, again, tricked into these calls and they are giving the information. I mean I would give information out too if Moffitt were calling me. I would think it would be legitimate.

So we have got to do something, and I appreciate you holding the hearing. And we are doing something, we are responding, so I appreciate it, in a bipartisan fashion. At the same time, again, Mr. Foss, at the same time, I do have concerns about legitimate, consented robocalls being inadvertently blocked. How often do legitimate calls inadvertently get blocked and how quickly can they be identified and remediated?

Again, I am concerned about the healthcare related robocalls where you remind an individual that their healthcare appointment is the following day or what have you. So, if you can give me an answer I would appreciate that.

Mr. FOSS. Yes, absolutely. So the other piece about like modern robocall blocking, we keep on saying the word "blocking" and "stopping" and, you know, the stopping at the network level, right, never letting those calls even get through, those should be for the ones that we are 100 percent guaranteed, we have proof, we have recordings, we have transcriptions, those can be stopped at the network level.

Even with Nomorobo, so on our landline product, if you are on our list you get a challenge question. It is called a captcha. You have to—it says this phone is protected by Nomorobo, please type the number 72, 6, right, humans can always get through. If a doctor's office is calling with a person that accidentally gets on, they can actually get through. It rings the number.

On mobile, we actually, since we are an app, we don't block the call. It just gets sent directly to voice mail, at which point even like with some of the newer phones it shows the transcription right

there. So, the risk of that message not getting through is actually incredibly small.

Mr. BILIRAKIS. OK, very good. Again, I appreciate the approach of better information sharing between FCC and industry in Mr. Latta's STOP Robocalls Act. I would like to work with him, he is a good friend, on more specific public-private partnership ideas as it continues through the process.

Mr. Foss, does your company have a working relationship with the Federal Communications Commission or the FTC to notify appropriate officials when you have specific identified bad actor, a bad actor, so they may review it for potential charges? If not, is this something you would consider?

Mr. FOSS. Yes, absolutely. So, our genesis, right, I won a competition from the FTC, right. We as a company, me as an individual, we owe them kind of a debt of gratitude. We are always willing to work with FTC, FCC, and law enforcement just in general. So, I can say that when we will detect a scam that is, let's say it is purporting to be from the FTC or from Social Security Administration or the IRS and things, we will reach out proactively to those organizations.

Right now, with the IRS one, we are making that automated. They can go and see the numbers that are actually going and doing that. What we found also works even better is working in reverse. So, think about the way that law enforcement has traditionally gone after these robocallers, right. They have to get subpoenas and subpoenas and kind of follow the traceback and going back and forth, and by that point the trail kind of goes cold.

I was on a panel with Consumer Reports and one of the attorney generals said that it sometimes takes up to 50 subpoenas to get one of these. What I encourage any law enforcement that reach out to us is we will tell you right now the calls that are coming through, right. You want to know the calls that are being made to people in Florida. You want to know the ones that are purporting to come from Florida or Texas or do you want IRS calls that are hitting people in Florida.

We have a honey pot, right, we have a quarter of a million phone lines that belong to us. We regularly send in real time those calls to law enforcement, so I have no idea what they do, right. Do they answer them? Do they trace them back? Do they—I don't know. But those kinds of partnerships and those kinds of teamwork, again, as part of that. And I have gone on record, right, there are a lot of public records where we have helped with a lot of those cases, gotten them shut down based on the data that we provided to law enforcement.

And again, we don't charge for any of that. That is just kind of part of our job is what we think.

Mr. HALLEY. If I could just add one thing to that which is that one of the reasons we set up the USTelecom Industry Traceback Group is to avoid the 50-subpoena problem. So, what we are able to do is rather than having somebody have to go to each individual carrier who may be in the call path and subpoena each of them individually, because the Communications Act provides for this we can do the whole traceback from involving every single carrier who is involved in that call without having to go through a subpoena

for each one of them. And we work very closely daily with the FCC and the FTC to provide referrals and provide that kind of information specifically to address that problem.

Mr. BILIRAKIS. Very good, thank you.

I appreciate it, Mr. Chairman. I yield back.

Mr. DOYLE. The gentleman yields back. The Chair now recognizes Mr. Pallone for 5 minutes.

Mr. PALLONE. Thank you, Mr. Chairman.

I wanted to start with Mr. Summitt. In your written testimony you note that Moffitt employees receive 6,600 external calls identified as coming from one of Moffitt's own internal numbers. And if I am understanding you correctly, you mean that Moffitt got 6,600 calls that were spoofed in what would seem to be an effort to trick employees at your hospital into believing that they were speaking to another employee when, in fact, it was a fraudster on the other end of the line; is that correct? Yes?

Mr. SUMMITT. Yes, sir. That is correct.

Mr. PALLONE. Can you explain why this spoofing of this type poses such a problem for your institution and for the security of a patient's information?

Mr. SUMMITT. Sure. There is a wide variety of those types of calls coming in and, quite frankly, when I mentioned this to our telecom people and we were reviewing the logs, they kind of chuckled because this is just one area and it is more than 6,600 of these calls. This is just one identifying themselves as Moffitt coming into Moffitt.

So, the reason this is dangerous is that internally if we are looking at our caller ID and we see someone from Moffitt calling, we are going to pick that phone call up. They have already won the first step in attempting to get information. And what they are doing is several different ranges of schemes going on. It will either be until I try to identify someone else in Moffitt that they can potentially get to by asking for a doctor by name and the location he is located in or a researcher by name to get into the research area, or they are actually asking information about patients and their patient information and their insurance information.

Mr. PALLONE. All right. Well, I appreciate that.

Now, Mr. Halley, your association, The Broadband Association has been in the forefront of bringing the telecom industry together to work on the robocalls problem. Under my bill, the Stopping Bad Robocalls Act, the FTC would issue rules requiring carriers to adopt call authentication technology like SHAKEN and STIR, and that tech would hopefully make it substantially more difficult for spoofing to continue on the scale that we are seeing today. So, can you explain how call authentication tech works and how it would help fix the robocall problem, please?

Mr. HALLEY. Yes, I would be happy to. And I am a telecom lawyer not an engineer, and luckily the people who are in charge of the STIR/SHAKEN protocol are all really smart engineers.

At a high level it involves inserting information into the headers involving calls and the exchange of tokens, essentially, between companies as call traffic, as a call traverses through multiple networks. And in a nutshell what it enables functionally is that when a call is originated, that originating carrier who is generating that

call is able to authenticate that the call is being made with a real number that is not a spoofed number. And then that carrier is telling everybody else in the chain, this is a legitimate call from a real telephone number that hasn't been spoofed.

And as long as everybody else in the call path has also implemented that protocol, it will continue to be passed from one carrier to the next with that information all the way to the end recipient.

Mr. PALLONE. Well, thank you.

And then my last question is to Ms. Saunders about autodialer. The FCC is currently considering how to interpret the definition of an autodialer that Congress adopted in '91. And, in my opinion, it is critical that the FCC put consumers first to ensure that robocallers aren't given a loophole to make more calls.

So, let me ask Ms. Saunders, what is the most important thing the FCC needs to understand when it comes to clarifying the definition of an autodialer and why is it important that we get our call authentication requirements right and we get this technology deployed?

Ms. SAUNDERS. The Telephone Consumer Protection Act is a consumer protection act. And given that, the FCC which implements the act should be required to implement its regulations and its interpretations to protect consumers, not to protect robodialers. The FCC currently has before it, dozens of petitions as I have mentioned requesting a loosening of the interpretations of autodialers in such a way that no autodialers currently being used would be covered.

So I think it is essential that the FCC remember that fact. It is clear from the litigation from the courts that there is a perfectly legitimate way to interpret autodialer to cover the autodialers that are being used so that consumers continue to be protected.

Mr. PALLONE. All right, thank you so much and I thank the panel. I thank you, Mr. Chairman.

Mr. DOYLE. The gentleman yields back. The Chair now recognizes Mr. Long for 5 minutes.

Mr. LONG. Thank you, Mr. Chairman. Thanks for holding this hearing.

Whenever people come up to me at home, there are two things that they want to tell me, which the other side of the aisle won't understand one of these things, the other one they can relate to. But they say, "Keep supporting Trump. Stick behind Trump. Support the President." That is always pretty much to a person what they say. The second thing that they say is, "When are you going to do something about these robocalls?" So, it might be different in other districts across the aisle, but that is the two questions. I imagine they probably get that second question.

And my staff yesterday when they were preparing for this hearing, they had a question for me. They said, "We are doing the robocall deal tomorrow. Tell us about some of the robocalls that you get." Well, the thought that popped into my mind was Elizabeth Barrett Browning's, "How do I love thee? Let me count the ways." How do I get robocalls? Let me count the ways. We all get a ton of robocalls.

But I have a question for everyone on the panel if you can help me with this, because this is a robocall that I get. It has slowed

down a little recently, but the total call, it is always a voice mail and it starts by "Or," with the word "Or," "Or to be placed on our Do Not Call list, press 2." Can any of you enlighten me what they are getting at or what they want? Or I have never pressed 2, I have always just pressed block call on my iPhone. But are you all familiar with that call and what is the scam?

Ms. SAUNDERS. So the Do Not Call Registry, which is a part of the Telephone Consumer Protection Act, requires that telemarketers ask—first of all, it prohibits calls unless you have consented in writing to the calls. But it also requires that they ask you if you want to be placed on their internal Do Not Call list. And if you answer yes, then they are required to put you on that list and prohibited from calling you again.

You are smart to not press 2, because that just alerts them that you actually are a live person and that they will call you again.

Mr. LONG. Well, that is all they are phishing for is the fact that you are——

Ms. SAUNDERS. Yes, they are phishing, because they are obviously already not complying with the law or they wouldn't have——

Mr. LONG. Well, there is no message. There is no, like, you know, for life insurance, a million dollars' worth of life insurance for a dollar a day, you know, press 1 to hear about that. The whole message is, "Or to be placed on our Do Not Call list, press 2." And I was just——

Mr. FOSS. Yes. So my thought here is that your—since you are saying it is going to voice mail, your voice mail message is probably pretty long. And so those autodialers will start playing the message when it detects, when it thinks that a person has picked up and said hello, and that is when it will start playing the message.

So if your message is, you know, "Hi, I am not here right now. If you need to reach me go over to here"——

Mr. LONG. I don't think I have a message. I think my mine is an auto message, but anyway.

Mr. FOSS. Well, whatever it may be, right? So that actually, if you answered that call you actually might find out the whole thing right there. This is the thing. Everybody thinks that these robocallers are like super smart and things. On the business side they absolutely are. On the blasting these calls out, it is just, you know——

Mr. LONG. While I have your microphone turned on there, on your Nomorobo what regulatory authority do you operate under?

Mr. FOSS. We don't, actually, right, there are none because we are a third-party service that the consumer is getting into a relationship directly with us.

Mr. LONG. And again, I know you have been asked this before, but how do you ensure legitimate calls go through with your service?

Mr. FOSS. Yes, so is it perfect? Absolutely not, right, our false positive last month was less than a tenth of a percent. And then we will go in, if we get reports then it will get on to our white list, our black list is automated. But, effectively, if the consumer doesn't like what we are doing, right, they cancel the service. They don't use it anymore.

Mr. LONG. And I think for Mr. Halley if they would have, if the staff would have just put on your card "Hal Lee," like Hal was your first name, Lee was your last name, everybody wouldn't have had a problem. But I recommend that for next time.

But, Mr. Summitt, before I run out of time here, I appreciate very much what you do in the cancer world. From a father of a Hodgkin's lymphoma survivor, I know how important those calls are that you get and how frightening it is when you are first diagnosed and you are expecting a call from the hospital.

Do you have any cause or should we have any cause for concern that when the hospital is calling to set up an appointment that we get that call instead of thinking that it is, you know, it may say your name on there and we think, well, that is a scam because we have heard it is a scam. Is there anything that we need to be cautious of or anything that we would vote on that we need to be sure and protect that your calls to remind people of appointments will get through?

Mr. SUMMITT. And I appreciate that question because that is one of our concerns is that I am afraid that if you are expecting a call from us and it turns out to be someone else and you have given away information, then I am just—then that problem is just going to add more to your problems that you have. And my concern is that those calls if it continues, they are going to stop.

So, my recommendation on anyone receiving any call from a healthcare organization is to call back the organization and make sure that it is a legitimate call.

Mr. LONG. OK, thank you.

Mr. Chairman, I am out of time. But if you want me to say anything later, just press 2.

Mr. DOYLE. I thank the gentleman. I polled our side. No one has ever got that first question asked of them.

The Chair now recognizes Mr. Veasey for 5 minutes.

Mr. VEASEY. Thank you, Mr. Chairman.

You know, one of the things that I have noticed that I thought was very interesting is that there are a lot of recommendations on here that would ask for providers and for telephone companies to make certain provisions that would make consumers less subject to these calls, requiring voice service providers to provide free effective caller ID authentication for all calls, requiring telephone companies to provide free call blocking services, establish an unblocking system that consumers can control calls, and submit regularly to the FCC about the implementation of some of these consumer protections.

But the question that I wanted to ask you is that when other industries like, for instance, in the alcohol industry where they have taken on, you know, anti-drunk driving, anti, you know, binging campaigns where tobacco companies have been required to make certain advertisements and what have you in efforts to prevent, you know, teens from smoking and to make their products, you know, less likely to fall into the hands of underage smokers, do you think that requiring telecom companies, not telecom companies but telemarketing companies, to maybe step up in this area and put money behind some of these campaigns dealing with call blocking and what have you would be a more effective way to go?

Ms. SAUNDERS. Is that for me?

Mr. VEASEY. Yes.

Ms. SAUNDERS. I appreciate the question. I think if we are unable to get telemarketers to comply with the law to even get consent before they call, I doubt whether we would actually be successful in getting them to pay the system to block their calls. I represent low-income consumers and I am very aware of the potential cost on small phone companies and their necessity of transferring those costs to the lowest income consumers who then would have trouble even affording their telephone.

We have not previously discussed this, but one idea that we have had, and I speak for a number of consumer groups, is that in recognition of the fact that my telephone is only useful if I can call many other people, the telephone system in the United States has long had a Universal Service Fund under which all telephone users contribute a small amount to support small telephone users' development and it has been used in a variety of ways.

We would suggest that the Universal Service Fund be investigated as a potential source of money for those very small companies or very poor phone companies to help them pay for the technology that would allow them to implement these protections. Because the entire system is only as strong as its weakest link and until we get all the systems in the country up to the same level, we are all vulnerable.

Mr. VEASEY. You know, I know that there have been certain States, my colleague here to the left, Representative Clarke, I know that her State of New York, that they have passed State legislation or attempted to pass State legislation to deal with this issue.

My question is that with this being an interstate commerce issue, is having a Federal law something that is really going to be required to really clamp down on this even more or do you think State laws on their own are effective?

Ms. SAUNDERS. So I have been involved with your colleagues in New York in working on the New York law. There are many similarities between that law and Mr. Pallone's law, bill, or I should say between the bills. I do think that unquestionably a Federal bill will be the fastest and most efficient way to deal with this problem.

Mr. HALLEY. I would agree with that. Whether it is in this context or another context, as a general matter on these sort of interstate communication services if we can have one national Federal framework to govern these issues I think that is ideal, so I would agree with my colleague.

Mr. VEASEY. And in closing with my last question here, until we can get these companies to, you know, to clean up their act and pass laws to prevent them from doing the spoofing and the unwanted calls, do you think that there needs to be more of a public education campaign?

One of the areas that really concerns me is senior, or senior citizens. I know that, you know, they obviously get targeted all the time. I know my grandmother died earlier this year. She was 106, she died earlier this year and, you know, she got numerous calls like all the time from telecom companies. Is there—but I don't see much out there as far as advertisements or public service announcements warning people about these calls.

Ms. SAUNDERS. If I might, I think public education is always valuable, but I have a personal situation where my very, very smart mother-in-law was taken in thinking that her grandson, my son, was calling her from Canada in jail. She was at the bank withdrawing money until someone—and she runs several businesses. So I am not sure that public education is something that we can rely on here.

Mr. VEASEY. That is amazing. OK, thank you.

Mr. Chairman, I yield back.

Mr. DOYLE. The gentleman yields back. The Chair now recognizes Mrs. Brooks for 5 minutes.

Mrs. BROOKS. Thank you, Mr. Chairman, and thank you for holding this very important hearing.

Ms. Saunders, I actually have a family member who had the same thing happen to him. And so, while education is critically important and strengthening our laws are really important, one thing as a former U.S. attorney I would like to talk about, because what hasn't really come up in any of the hearings so far is where has law enforcement been in all of this.

And I am very curious, and that is what one of the bills, H.R. 721, is a Spam Calls Task Force Act. But what I am really curious about, and I think, Mr. Halley, in your testimony, in your written testimony you talked about the Justice Department and we need more criminal enforcement actions. Is it happening? Are U.S. attorneys and the Justice Department, have they in the last 8 years, to what Mr. Summitt's point it has really accelerated in the last 8 years. Can we point to any cases? Has anyone gone to jail, been prosecuted?

These may be complex cases, because they may involve national actors and international actors and does anyone know about anything relative to that? Mr. Halley?

Mr. HALLEY. So the short answer is not enough is happening. We are seeing a lot of efforts out of the Federal Communications Commission through forfeiture penalties and going after companies who are breaking the law. Even in that instance, you know, when somebody fails to pay their fine it is incumbent upon the Department of Justice to go collect the funds, so there is more work that could be done there.

But also——

Mrs. BROOKS. Those would be civil forfeiture sentences.

Mr. HALLEY. Exactly. So, on the criminal side, not—no, there hasn't been a sufficient amount of activity to go after criminal actors. The FTC has a separate authority. They have also taken a significant amount of actions on the civil authority side, but there has not been a sufficient focus on folks who are, you know, blatantly illegally breaking the law, committing fraud, et cetera, in my opinion.

Mrs. BROOKS. I assume they may be very difficult cases to put together. Does anyone know about any cases?

Ms. Saunders?

Ms. SAUNDERS. The FTC has brought 151 cases in the last 10 years.

Mrs. BROOKS. Criminal cases?

Ms. SAUNDERS. No, civil cases.

Mrs. BROOKS. OK.

Ms. SAUNDERS. The FCC has brought a smaller number. I would posit that unless you can get the criminal cases instigated, and unfortunately U.S. attorneys and district attorneys are generally more concerned with going after different kinds of crimes——

Mrs. BROOKS. I understand.

Ms. SAUNDERS [continuing]. That the best enforcement is private enforcement. It is not popular, but if you arm individuals who have been harmed by these scams and by these unwanted calls with the ability to go into court and force the people who have been harassing them to pay penalties, that creates at least a financial incentive to comply with the law. That is for the non-scam calls.

So, I agree with what has been said that the only way you are going to deal with the scam calls is to criminally prosecute them. But it is about half and half.

Mrs. BROOKS. Any other comments, Mr. Foss?

Mr. FOSS. Yes.

Mrs. BROOKS. On criminal enforcement?

Mr. FOSS. I am a big fan of an ounce of prevention, right, rather than a pound of cure. It seems like enforcement to me is the pound of cure. If we were to put an ounce of prevention into the network level, I think that we would see a marked reduction in these predatory scams.

Mrs. BROOKS. Mr. Summitt, I have a question because you have been a cyber expert for a long time, can you share with us though how—what your concerns are particularly with hospital cases and with hospital systems? Is the primary concern the identity theft that is taking place or is the primary concern that—because I think, you know, the Justice Department has been involved in the past, and long in the past when I was in the Justice Department from '01 to '07, we were very focused on identity theft.

And I am just curious whether, you know, are you hearing from your patients and others that it is the identity theft or is it actual, has any patient care actually been impeded?

Mr. SUMMITT. It is across the board, Congresswoman. Patient relationships with our providers and the patients themselves are being impacted. The trust factor is there. We have people that have heard the worst news of their lives coming into our organization and to add on top of that anything else is not going to go well for that patient. So we see this as absolutely affecting patient safety and patient care especially when it starts interrupting our workers inside the facility by receiving these calls and then having to deal with them.

There are so many different avenues that this is impacting that this is why I am excited that we are finally getting—that I am able to give you the idea of what is going on in the real world right now.

Mrs. BROOKS. Thank you. I think we need the prevention beyond the cure. I yield back.

Mr. DOYLE. I thank the gentlelady. I would note that the Wall Street Journal reported that the FCC levied $208 million of fines against telemarketers. They have collected $6,790 of that 208 million. Remind them not to ever hire them for my debt collectors.

The Chair now yields 5 minutes to Mr. Soto.

Mr. SOTO. Thank you, Mr. Chairman. And during this committee hearing I received a robocall myself. Thanks for recognizing that we are all being inundated by these calls. Apparently, if you own property in Florida there are lots of real estate speculators who want to buy it. I guess that is a good sign for my district at least.

If we can talk about one thing that is definitely bipartisan, it is annoying robocalls. We have heard it throughout so many of my colleagues today, but particularly when we are talking about it being sort of the presupposed fraud and crime it becomes a big issue. You know, we are particularly honing in in my office on fraudulent healthcare calls and one of the, I think one of the budget submissions we have submitted on healthcare is to the Federal Trade Commission on fraudulent healthcare calls.

The committee is aware of growing practice of robocallers targeting healthcare providers and patients in an effort to commit financial fraud. In some cases, callers use spoof numbers making it appear like they are calling from a hospital or a physician office and seek to obtain sensitive health-related or other financial information about patients. It goes on from there.

But I want to thank one of our guests today who work with us to help put that together. That is Mr. Dave Summitt, thanks for being here today. You are the CIO overseeing cybersecurity at H. Lee Moffitt Cancer Center in Florida, so welcome up from our State. One of the busiest cancer centers in the United States, ranked by U.S. News and World Report as one of the top ten cancer centers in the United States and you are under constant attack by this, attempts to get people's health information.

So, would language like that be helpful in moving the FTC along to help partner with you in this area, and how are they doing right now as far as helping with what you are trying to achieve to protect people's information at Moffitt Cancer Center?

Mr. SUMMITT. So, Congressman, just clarification, I am Chief Information Security Officer at Moffitt.

Mr. SOTO. Oh, we gave you a raise there.

Mr. SUMMITT. You gave me a raise. Thank you, I appreciate that and hope the people back home are hearing this.

Mr. SOTO. Chief Information Security Officer, OK.

Mr. SUMMITT. And now I have kind of lost the question.

Mr. SOTO. So how is the—would language like this directing the FTC to particularly hone in on fraudulent calls related to healthcare be helpful and how have they been partnering with you currently?

Mr. SUMMITT. I wish I could say that we are combating this effectively on a daily basis. But we are so inundated with this particular problem and the other problems that we have just in cyber on networks and network attacks and software attacks that we just do not have the bandwidth to sit and do this on a daily basis. That is the damaging part of this. We cannot combat this alone.

I do believe that these bills that I have been reading has a lot of great things in each one of them that when we start working together here, we are going to be able to solve this problem. And I do believe we have the technology right now to solve this problem, if not heavily curb it. I would like to see some more activities specifically within our critical infrastructure and healthcare to have

additional tools on our behalf to help us with this fight. And I do believe the FCC and the FTC can absolutely step up and help us out with this along with the telecoms and along with the third parties. But, so one single solution isn't the answer here.

Mr. SOTO. Thank you, Mr. Summitt.

Now I recently was able to block some of those calls I was getting about these real estate solicitations. I just want to, for the record, for Ms. Saunders, Mr. Halley, and Mr. Foss, what phones don't have a blocking function and how do you feel about requiring all new phones to have a blocking function?

We will start with you, Ms. Saunders.

Ms. SAUNDERS. My understanding is that most landlines do not have a really robust blocking function.

Mr. SOTO. OK. Is that a consensus among all of you?

Mr. FOSS. Yes.

Mr. SOTO. Are there other types of phones that don't have a blocking function right now?

Mr. FOSS. Also like feature phones, flip phones that are, you know, old school cell phones. The modern smartphones from Android, from Apple, those operating systems allow app developers to build those in. But effectively any other device, nothing is built in.

Mr. SOTO. So these are really where the battle lines are formed.

Mr. Halley?

Mr. HALLEY. I was going to say, but that doesn't prevent carriers from trying to build in network blocking solutions so that the call never actually gets through, regardless of what kind of device the consumer has. And we are actively working on those types of solutions as well.

Mr. FOSS. Even for it is at the network level where they are piggybacking off of certain services like caller ID to go and show an indicator that it is a robocall, at least that is giving information to the landlines that would say something like "robocaller," or to the feature phones. So yes, don't let the perfect get in the way of very good.

Mr. DOYLE. The gentleman yields back. The Chair now recognizes Mr. Walberg for 5 minutes.

Mr. WALBERG. Thank you, Mr. Chairman, and thanks to the panel for being here.

And I keep my smartphone out here to see what is going to come in here as a spoof. My carrier, I know, catches a number of calls, but I regularly keep this to remind myself that the spoof does come in. I don't get to answer many of the calls that come through. I choose to let them go to voice mail if it happens, and most don't. So, this is an important hearing and a hearing that hopefully solutions will come because this is a great tool, but it is sure wasting our lives in many ways.

Today's hearing is a great start in addressing this growing problem. There are several bills on today's hearing which each add different ideas to the conversation. While this is promising, we need to remain focused on the larger problem first as we piece together legislation. Illegal spoofed calls, not calls that may be legitimate, but unwanted, it is critical that we not conflate the two.

Mr. Halley, the STIR/SHAKEN standards that telephone carriers are implementing is a great first step at tackling clearly illegal

spoofed calls. As we try to capture other types of spoofed calls in addition to nonexistent area codes or unassigned numbers, how do we stop bad actors while maintaining flexibility and consumer choice?

Mr. HALLEY. Thank you for the question. So, implementation of STIR/SHAKEN across the network is critically important as you have just identified. The other things we can do are making the types of analytics tools, whether they are provided in our carriers' networks or over the top, available to as many people as we possibly can.

And the other third piece I would mention, two others, really, one is the Industry Traceback Group, making sure that all companies are participating in the Industry Traceback process. And one thing I should say is, you know, Mr. Summitt has suggested that there are solutions to solve this problem and I agree. Not everybody participates in the traceback process, all right. There are times when we initiate a traceback and we can figure out the call ended at carrier A who received it from carrier B, and then when we get to the next one in the chain, they are not a part of a group, some of them refuse to participate and so that is a problem.

And so, efforts via the legislative process to provide more information and to encourage participation in that traceback process would be really important. And as I have said, in addition to that, sort of going after the root of these illegal robocalls and putting some folks behind bars would be a helpful solution as well.

Mr. WALBERG. Along that line, with technology constantly advancing faster than we can really keep up with it, how do we ensure that our regulations as well keep up with advances in technology?

Mr. HALLEY. So to me the key is flexibility and not over-prescription, because whatever the current standard is it is going to be different 5 years from now because we will have learned the way in which people try to get around it and we are going to need to as an industry be able to quickly and flexibly update the protocols and update the processes in which we operate. And so, to me, the thing we need to be careful about is just that if we are going to have any sort of requirements whether they be congressional or FCC that we do so in a manner that ensures sufficient flexibility for industry, because even we are going to have trouble keeping up with the bad guys. Certainly, government is going to have trouble as well.

Mr. WALBERG. OK, Mr. Foss, would you like to add something to that?

Mr. FOSS. Yes, absolutely. I would caution on any of these laws and regulations, right, don't get into the weeds. Let us get into the weeds. Even Mr. Soto was asking, do we need to make certain exemption or focus on healthcare and things like that, like let us do the heavy lifting. If you do a broad definition, what is an autodialer, what is a violation, when does that occur, that would be really, really helpful for all of us.

Mr. WALBERG. Mr. Summitt?

Mr. SUMMITT. Yes. And I would also add to that not just you guys get in the weeds, get us involved in the community and in these businesses and in our critical infrastructure as part of that discussion, I think, is just so very, very important. I think the sup-

port of the task, 721, the task force, is going to be a great thing in moving this forward and that is where you get the interagency together and that is, I believe, one of the key things in getting your legislation defined here.

Mr. WALBERG. Mr. Halley, are there any things that you see in specific that aren't in these bills that we are meeting around today?

Mr. HALLEY. Yes. So, I think we are supportive of the objectives of the legislation generally across the board. There are certain details which we might offer suggestions, and we have had productive conversations with the staff or the sponsors in the committee and we appreciate that opportunity and we will continue to have that discussion.

Mr. WALBERG. Thank you. I yield back.

Mr. DOYLE. The gentleman yields back. The Chair now recognizes Mr. O'Halleran for 5 minutes.

Mr. O'HALLERAN. I thank you, Mr. Chairman, for convening this important hearing to examine some forms of abuse of robocalls—I'm sorry—consumers in my district receive daily and I do too. In fact, I was thinking we don't even answer the phone anymore whether it is cell or landline if we don't know the number. We will look it up on the computer and check it, but we just don't do that anymore.

I often hear similar concerns from Arizonans about this issue. As a former small business owner, I recognize that businesses have certain reasons in which they need to contact customers for legitimate purposes. As a former law enforcement officer, I also recognize there are bad actors today trying to scam consumers and these bad actors need to be held accountable for their actions. While some bad actors may be based beyond our borders, we need to ensure our Government has the resources it needs to protect Americans nationwide.

Mr. Halley, I would like to recognize and commend the industry for taking proactive steps to develop call authorization technology to stop the influx of unwanted robocalls. While STIR/SHAKEN tools are starting to be adapted by carriers, in your view, do smaller wireless carriers in rural communities face any roadblocks to adapting these new technologies?

Mr. HALLEY. Well, the protocol is the protocol regardless of who the provider is, but I will say that there is a cost, right, associated with implementing the software and upgrading your network. As a general matter, when new technology is rolled out among, you know, the entire industry, you know, advancements tend to happen faster with the larger providers first, and sometimes there are issues of equipment availability and vendor availability.

So I think we need to be on the lookout for making sure that solutions are available on a timely manner and in a cost-effective manner for all providers, but particularly with the smaller providers where that may be a problem.

Mr. O'HALLERAN. Thank you. And also, Mr. Halley, in your testimony you state that there are acute need for aggressive criminal enforcement against illegal robocallers at the Federal and State level and that fines alone are insufficient. How can section 5 of H.R. 946, of which I am a cosponsor, be enhanced to provide broader enforcement for robocall violations?

Mr. HALLEY. Sure, so the legislative efforts here that are looking at enabling folks to go after first-time offenders, I think, is positive consideration, of increasing the forfeiture penalties is something definitely that should be looked at. I will say with respect to the FCC's collection issue, one of the challenges they face, just to give them some credit, is they can issue forfeitures, but once somebody decides not to pay it, they are then dependent on the Department of Justice to go after those bad actors in court which sometimes can create an issue.

So, I think the way that it can be advanced would be to recognize that in addition to things we can do on the civil enforcement side, there may be things we can look at whether it is, you know, directing the Department of Justice to form a specific group to specifically go after illegal robocallers that are committing fraudulent activities, for example. I do agree that the legislation that is looking at requiring the Attorney General to lead an interagency effort is a potentially positive step as well.

Mr. O'HALLERAN. And just as an aside here, there has been so many times in our history as a country whatever the issue is that we talk about enforcement, but we really, truly don't get down to enforcing because of the complexity of the system or the lack of personnel or the lack of funding, whatever it is. We can talk all day, but if we don't know how to enforce it and really put the funds forward, then we are just telling the consumer out there that we really don't want to get this dealt with.

Mr. Summitt, I just want to thank you for sharing your compelling testimony with us on the difficulties your organization faces with the influx of robocalls you receive while you are trying to focus on your mission of saving lives.

Mr. Chairman, I believe we have a duty to bring relief to consumers who have been the victims of malicious robocalls from bad actors. I look forward to working with my colleagues on legislation like H.R. 946 to address this pervasive issue once and for all. And I yield back.

Mr. DOYLE. The gentleman yields back. The Chair now recognizes Mr. Gianforte for 5 minutes.

Mr. GIANFORTE. OK, thank you, Mr. Chairman. I thank the panelists for being here today for this important topic. Montanans reasonably think that being on the National Do Not Call List means they won't get called, except they are getting called, a lot, and they are sick and tired of it.

Alvin, a 70-year-old man from Kalispell, receives over 20 calls a day. His provider allows him to block 12 numbers; clearly that is not enough. Connie in Missoula asked me to get back to her about an issue by email, not by phone. Why, because she is getting inundated with robocalls and doesn't pick up her phone. A young woman in Bozeman received a call from her little brother's phone number, but it wasn't her brother. It was a scammer calling from her little brother's number. Unfortunately, her little brother had died of a heroin overdose a couple of months previously. She was shaken and shocked.

It is an indictment on the system that a young woman gets a call from a scammer using her deceased brother's phone number. I look forward to solutions and I am encouraged by the conversation

today to end this practice so no one has to go through what this young woman did. There is a bipartisan agreement here and I think this needs to be fixed. I look forward to working together with my colleagues to get it fixed.

So, I want to focus, continue the conversation on law enforcement and what we need to do to help, and I will start with Mr. Halley. You mentioned the need for increased criminal enforcement in this area to quickly crack down on bad actors. Can you explain what you think can be done to better empower law enforcement to go after bad actors?

Mr. HALLEY. Sure. Look, there is the TCPA. There is the Truth in Caller ID Act. There are other consumer protection, you know, fraud prevention laws that are on the books. I think as much as anything it is not so much that we need to change the law as it is that we need to recognize that if this is, in fact, such a big issue, it is not just a nuisance issue, right, it is a real issue that affects not just healthcare institutions but banks and many other industries as well that are having similar problems, we need to recognize that.

It is not just about a nuisance. It is about real crime, real fraud. And for those types of calls, I think we just need to sort of double down and quadruple down on our commitment to actually enforce laws and go after those who are committing crime.

Mr. GIANFORTE. OK.

Mr. Foss, would you like to add anything to that?

Mr. FOSS. Yes, so this kind of a forum, the enforcement side doesn't seem to be working as strongly as the prevention side. So, I would just, you know, do we need all the prongs of this, absolutely. I don't know, I don't have any specific recommendations over there, right. The things that I always usually suggest are looking at this problem from different angles, right, looking at with the new technology. Don't look at it, this is a very different type of crime that is being perpetrated. It has been traced back and things need to change nowadays, and again things that like USTelecom are doing and things and having new tools like our honey pot and things like that. I think that we can absolutely do that.

Mr. GIANFORTE. OK.

Mr. HALLEY. I would just say we can probably do more and we are now doing more also at the State level, really coordinating with State Attorneys General as well for particular incidents that are going on within the State borders.

Mr. GIANFORTE. OK.

Mr. Summitt, anything you would add?

Mr. SUMMITT. Sure. Technology can solve a lot of things, but it can't—it is not the end-all. It is not a hundred percent. And as much as I would like to agree, I would respectfully disagree with enforcement. Even though enforcement has not been as effective as it can be, I think the reason is we don't have enough information going forward to prosecute some of these things.

And, quite frankly, when I am getting 6,600 calls in a 90-day period, I can't do a traceback on 6,600 calls nor does a telecom want me to give them every time this happens. So, enforcement side of

this and getting the latitude to the FTC to pursue with cooperation from us providing data to them is a key part of this.

Mr. GIANFORTE. OK. And again, I want to thank the panelists for being here today for this important topic. And with that, Mr. Chairman, I yield back.

Mr. DOYLE. The gentleman yields back. The Chair now recognizes Ms. Eshoo for 5 minutes.

Ms. ESHOO. Thank you, Mr. Chairman. And I apologize to the committee members and to those that are testifying that I haven't been able to be here for most of the hearing. I am chairing a hearing upstairs on the cost of prescription drugs in Medicare.

What I am struck by is that the United States of America saw to it that a man landed and walked on the moon in 1969, the year my first child was born, and I just can't accept the fact that we can't really rid people of the harassment of robocalls. I do believe in technology and I think that enforcement and technology together are the set of bookends that we need in this.

To Ms. Saunders, in your written testimony you say that the NCLC supports the HANGUP Act which I am very grateful for. As I mentioned in my opening statement, the Fourth Circuit Court of Appeals decided that the loophole that my bill repeals is unconstitutional. Can you just spend a moment on why there is still a need for the legislation now that the Fourth Circuit declared the loophole unconstitutional?

Ms. SAUNDERS. Yes, thank you, Ms. Eshoo. The HANGUP Act would undo a really grievous harm to the TCPA which exempted all calls made to collect Federal Government debt from the requirement of consent. We have seen, I would say, hundreds of cases by student loan collectors, generally, who are harassing not just borrowers, but also friends and neighbors and wrong number calls with unmercifully high number of calls. And we have actually even submitted a complaint to the FCC asking them to deal with it which they have not.

Ms. ESHOO. What was their response?

Ms. SAUNDERS. None.

Ms. ESHOO. Ah.

Ms. SAUNDERS. There was no response.

Ms. ESHOO. There you go.

Ms. SAUNDERS. So we strongly support the HANGUP Act.

In response to your specific question, we have 11 circuits in this Nation, one circuit has not declared the TCPA's provision exempting these calls from the consent requirement as unconstitutional. But the callers themselves routinely defend actions brought against them for illegal robocalls by saying this whole statute is unconstitutional and that was the goal in this case. So, this good decision in the Fourth Circuit may not stand. It may be overruled en banc. It may be overruled by the Supreme Court and may be differed with by other circuits. The HANGUP Act is still essential.

Ms. ESHOO. Thank you very much.

To Mr. Foss, thank you for—I read your written testimony and I loved how you just came to the point. Usually written testimony is encyclopedic and so yours was just a pleasure. It was like I just turned the page once or twice and I was done. But there was a lot packed into it.

Mr. FOSS. I just get down to business. I don't know.

Ms. ESHOO. Yes, how do you deal with spoofing? So, specifically, if a robocaller uses my phone number to mask their identity, would your technology blacklist my phone number even though I haven't robocalled?

Mr. FOSS. No. So, we don't really care if a phone number is spoofed or legitimate, it is real, we care about the calling patterns. So, in that case, if somebody spoofs your number and is now making, you know, tens of thousands of calls in an hour, well, then it is going to get on our blacklist while that attack is happening, right. Once that attack, once they go on to someone else's number it drops off our blacklist and there is no harm with that.

Ms. ESHOO. So your blacklist deals with volume?

Mr. FOSS. Correct, because that is the best—volume as well as content. So again, if we see a small volume but we have a recording, we have a transcription, we know what is going after that, that is one way that your reputation will go down. The most obvious way is just when you start seeing these high-volume calling patterns.

Ms. ESHOO. I see. Well, thank you for your important work.

To Mr. Halley, much has been discussed today or I think it has given the testimony about the problems with voice-based autodialers. What are your members doing to ensure that Americans still have landlines that are protected from robocalls?

Mr. HALLEY. Sure, so we are building——

Ms. ESHOO. There are still a lot of people that have them.

Mr. HALLEY. Absolutely, there are.

Ms. ESHOO. I know my kids don't understand it at all, but——

Mr. HALLEY. Right. No, I have one and it is an old 1980s-style phone and my son just looked at it and started to talk into it, and it didn't work. It was pretty funny.

Anyway, we are doing a lot. So, we are building in technology into our network so that even if the phone itself, for example, is an older phone, the network has the capability to block calls that are unwanted or illegal. And, you know, we are looking at solutions like anonymous call rejections services for those types of older services where if the number, if somebody who is calling has specifically stripped their caller ID, it won't go through.

Ms. ESHOO. How much of a dent do you think, I mean the universe, say, is a hundred percent robocalls on landlines, what would you estimate what you have done has put what percentage of a dent into it?

Mr. HALLEY. Well, you have to start with the percentage of calls that are over landline which are——

Ms. ESHOO. I understand.

Mr. HALLEY [continuing]. Extremely small. So, for that remaining portion of calls that do come over land——

Ms. ESHOO. It is a lot to people that just have a landline though.

Mr. HALLEY. Of course, for those individual callers, sure. You know, look, for those people who have opted in to the solutions that I am talking about it has made a huge dent. The calls either don't get through or they have a lot more information about the call so that they can make a decision as to whether or not they want to answer it or not.

In terms of whether or not, you know, 10, 20, or 90 percent of customers have actually taken those services, I don't know, but it is rising every day.

Ms. ESHOO. Thank you.

Thank you, Mr. Chairman.

Mr. DOYLE. The gentlelady yields. Ms. DeGette, you are recognized for 5 minutes.

Ms. DEGETTE. Thank you very much, Mr. Chairman. I was up at a hearing in Natural Resources and I apologized to them for being late because of I was here earlier. And everybody in the room on both sides of aisle says, "We need to do something about robocalls." So this is something that I think that is striking everybody in America.

And I have always wondered about what, exactly what the Do Not Call Registry did. And I also think, and I am just going to say this in public, I think that the Do Not Call Registry had real benefits but it had some real shortcomings. And, in my opinion, one of the shortcomings that it had is it allowed campaigns to exempt themselves. So, I get called on a frequent basis by candidates wanting me to record robocalls for them to send out and I won't do it because I think that robocalls by politicians maybe should be even more illegal than robocalls from everybody else.

But in any event, that is what I want to talk to the panel about today is the national no call registry because it seemed like it was making some real impact for a while, but now it seems that—and even at its most effective points consumers didn't realize things like politicians and others could still make calls under the Do Not Call Registry. And I am wondering if we pass some of this legislation that we are considering today, are we going to have some of the same shortcomings that we have found with the Do Not Call List?

So, Ms. Saunders, I wanted to ask you, do you think that Congress and the FTC did enough to prepare the public for what the Registry would and wouldn't do?

Ms. SAUNDERS. I am afraid that I am not familiar with exactly what the FTC and the FCC did years ago.

Ms. DEGETTE. OK.

Ms. SAUNDERS. I can tell you—I can answer more about what is currently going.

Ms. DEGETTE. Tell me what is—yes, well, tell me about the current situation.

Ms. SAUNDERS. So I think the Do Not Call Registry is good if it could be enforced.

Ms. DEGETTE. Right.

Ms. SAUNDERS. Unfortunately, there is the—the private remedies for enforcing it are not nearly as good as the private remedies for enforcing the rest of the TCPA. Senator Durbin on the Senate side is proposing a bill that will make the remedies somewhat equivalent. The FCC has the authority to expand beyond telemarketing and include other calls in the prohibition to landlines. They could potentially do that or one of the bills that are pending today could allow that expansion.

Ms. DEGETTE. Right.

Ms. SAUNDERS. The New York bill that is currently pending would prohibit all automated calls and prerecorded calls to landlines and residential, to landlines and cell phones and business phones, regardless of content if they are automated, unless there is consent or there is an emergency. So, there are different things that can be done.

Ms. DEGETTE. What would you think would be the—not commenting on the specific bills, but what kind of a paradigm would be the most important paradigm for consumers, do you think, for Congress to pass?

Ms. SAUNDERS. I think that has been recognized here today we are dealing with two sides of a problem. We have three kinds of calls that are being made——

Ms. DEGETTE. Right.

Ms. SAUNDERS [continuing]. To borrow Mr. Foss' analysis. One are the wanted reminders and legitimate business calls that we want to make sure are allowed through. For those calls, as long as consent has been provided there is no problem. Then on the other side are the scam calls which whether that is 30 percent or 47 percent, clearly, they need to be stopped.

Ms. DEGETTE. Right.

Ms. SAUNDERS. That is probably best stopped with a caller authentication problem and the technologies that Mr. Foss and others implement. For the rest of the calls which 30, 40 percent, those are telemarketing and unwanted debt collection calls, we need a very strong Telephone Consumer Protection Act that will create the financial incentive for the callers to comply with the law. In the meantime, with call authentication and effective tracebacks we will be able to catch them because we will know who they are.

Ms. DEGETTE. So, Mr. Halley, do we have the technology to be able to carry out that kind of a paradigm?

Mr. HALLEY. Yes, we do.

Ms. DEGETTE. Mr. Foss is also nodding yes.

Mr. HALLEY. Yes, we have the technology. Now what is incumbent on some of the things that I have been talking about today is carrier participation. So USTelecom members actively participate in tracing back calls, for example, not all of them do and not every carrier is necessarily implementing, you know, all the different tools and solutions that we are talking about. The technology is there, but we do have to make sure that everybody who is part of this is taking advantage of it.

Ms. DEGETTE. Thank you.

Thank you very much, Mr. Chairman. I yield back.

Mr. DOYLE. The gentlelady yields back.

Without objection, the following documents will be made part of the record: A letter from the Chamber of Commerce Coalition members; a letter from Consumer Reports; a letter from the Electronic Privacy Information Center; a letter from National Association of Federally-Insured Credit Unions; a letter from ACA International; an attachment to the letter from ACA International; and a letter from Representative Van Drew of New Jersey. Without objection, so ordered.

[The information appears at the conclusion of the hearing.]

Mr. DOYLE. I want to thank the witnesses for their participation in today's hearing. I want to remind all Members that, pursuant to committee rules, they have 10 business days to submit additional questions for the record to be answered by the witnesses who have appeared. I ask each witness to respond promptly to any such question you may receive.

At this time, the subcommittee is adjourned.

[Whereupon, at 12:15 p.m., the subcommittee was adjourned.]

[Material submitted for inclusion in the record follows:]

ctia™

Meredith Attwell Baker

April 29, 2019

Honorable Robert Latta
Ranking Member
House Committee on Energy & Commerce
Subcommittee on Communications & Technology
2322 Rayburn House Office Building
Washington, D.C. 20515

Dear Congressman Latta:

CTIA and its members work to prevent consumers from receiving irritating, intrusive and illegal robocalls, collectively stopping more than a million calls every day. That is why CTIA applauds your discussion draft confirming the ability of wireless companies to help prevent unwanted calls from reaching consumers, and aiding the FCC to pursue those wrongdoers.

Specifically, language allowing voice providers to provide robocall blocking on an informed opt-out basis makes clear that wireless companies help prevent robocalls from reaching consumers, particularly in combination with the draft's language that confirms providers can block calls as permitted by law. Additionally, when robocalls or spoofed calls do reach carriers' customers, the concept of ensuring that the FCC has established a streamlined process for a private entity to share information about those calls will help the FCC pursue robocallers that violate the law.

Thank you for your work to help stem the tide of intrusive robocalls, and CTIA looks forward to continuing to work with you and your colleagues on this important issue.

Sincerely,

[redacted]

Meredith Attwell Baker
President and CEO

1400 16th Street, NW · Suite 600 · Washington, DC 20036 · www.ctia.org

AMERICA'S COMMUNICATIONS ASSOCIATION

#ACAConnects

Matthew M. Polka, President and CEO
Direct Dial: 412-922-8300, Ext. 14
E-Mail: mpolka@acaconnects.org

April 29, 2019

The Honorable Mike Doyle
306 Cannon House Office Building
Washington, DC 20515

The Honorable Bob Latta
2467 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Doyle and Republican Leader Latta:

On behalf of ACA Connects—America's Communications Association ("ACA Connects"), I applaud the Subcommittee on Communications and Technology for its work to identify legislative solutions to the problem of robocalls. ACA Connects is pleased that, at tomorrow's legislative hearing, the subcommittee will consider a discussion draft – the Support Tools to Obliterate Pesky Robocalls ("STOP Robocalls") Act – that would affirm that ACA Connects members and other voice service providers can give their customers free robocall blocking tools on an informed opt-out basis.

Like other providers, the small and medium-sized operators of ACA Connects know all too well the burdens and frustrations that robocalls impose on their customers. Today, many ACA Connects members provide robocall blocking tools that they enable for customers on an opt-in basis. While those customers that use these tools generally find that they provide substantial relief from robocalls, relatively few customers take the affirmative step to opt in. Customer groups that are less familiar with new technologies may be particularly unlikely to sign up, even though these customers may benefit the most from protection against nuisance calls and malicious scams.

By moving to an "informed opt-out" model as the STOP Robocalls Act contemplates, a provider can empower a much broader share of its customers to enjoy freedom from robocalls—while still preserving the right of the customer to choose. Broader penetration of robocall blocking tools may also help a provider better differentiate its voice services in today's competitive marketplace. Benefits like these can make it easier, especially for smaller providers, to justify the costs they incur to provide these tools in the first place. Giving providers this flexibility would be a "win-win" for providers and customers alike.

We all know that there is no one solution to the robocalls problem. Stakeholders must continue to work creatively and cooperatively across many forums, and ACA Connects is proud to be an active participant in these efforts. The "opt-out" provision of the STOP Robocalls Act is an important step in the right direction, one that will help "move the needle" for America's consumers. We thank the committee for considering the STOP Robocalls Act discussion draft, and we encourage it to advance legislation as soon as possible that affirms providers' ability to offer free robocall blocking on an informed opt-out basis.

Respectfully,

[redacted]

Matthew M. Polka
President and CEO
ACA Connects – America's Communications Association

cc: Members of the House Committee on Energy and Commerce, Subcommittee on Communications and Technology

April 29, 2019

The Honorable Mike Doyle
306 Cannon House Office Building
Washington, DC 20515

The Honorable Bob Latta
2467 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Doyle and Republican Leader Latta:

The undersigned are competitive providers of interconnected VoIP and other voice services. We write today to thank the subcommittee for considering the Support Tools to Obliterate Pesky Robocalls ("STOP Robocalls") Act discussion draft, which includes a provision affirming that voice providers may offer free robocall blocking tools to new or existing customers on an informed opt-out basis. This provision would empower providers like us do more to shield our customers from the ceaseless torrent of robocalls.

There are effective tools available today that block robocalls before they reach the customer. We provide such tools to our customers on an opt-in basis at no cost. However, in our experience, notwithstanding our efforts to inform our customers of the significant benefits of these tools, relatively few customers take the affirmative step of signing up for them. These low opt-in rates persist in spite of consumers' growing frustration with robocalls. And the feedback we've received from "early adopters" of robocall blocking tools has been overwhelmingly positive, which makes it unfortunate that customers who are less familiar with and slower to adopt new technologies are missing out.

We could help more of our customers enjoy the benefits of free robocall blocking if we offered these tools on an informed opt-out basis, as the STOP Robocalls Act would allow us to do. Given the popularity of these tools among customers that use them, we anticipate that opt-out rates would be low—and thus, many more of our customers would receive the benefit of these tools than do today. The result would be a significant net improvement in our customers' user experience. And the more widely our customers use these tools, the better these tools can help us differentiate our voice offerings in today's highly competitive marketplace.

Every day, our customers are bombarded with robocalls. We want to do more to help them protect themselves from this onslaught, and the "opt-out" provision of the STOP Robocalls Act discussion draft will enable us to do just that. We encourage the subcommittee to give this provision its fullest consideration.

Respectfully,

_____/s/_____
Jonathan Bullock
VP, Corporate Development and Government
Hotwire Communications

____/s/___
Joe Canavan
Chief Operating Officer
Blue Stream

_____/s/_____
Michael Candelaria
General Manager/CEO
Mid-Rivers Communications

_____/s/_____
Katherine Gessner
President
MCTV

____/s/___
Lee Haefele
President
Haefele Connect

___/s/___
Tara Kelley
SVP, White Label
Momentum Telecom

_____/s/____
Travis Kohlrus
VP, Broadband
Eagle Communications, Inc.

_____/s/_____
Robert M. Wieand
Chief Financial Officer
Service Electric Cablevision

cc: Members of the House Committee on Energy and Commerce, Subcommittee on Communications and Technology

April 29, 2019

The Honorable Michael Doyle
Chair
Subcommittee on Communications
and Technology
U.S. House of Representatives
Washington, DC 20515

The Honorable Robert Latta
Ranking Member
Subcommittee on Communications
and Technology
U.S. House of Representatives
Washington, DC 20515

Dear Chairman Doyle and Ranking Member Latta:

The undersigned organizations, which represent a diverse group of industry sectors throughout the economy, write regarding the Communications and Technology Subcommittee's upcoming hearing on the problem of illegal automated calls. Thank you for scheduling this important hearing. We strongly support and share the goal of thwarting unlawful actors that seek to defraud or commit other unlawful acts against consumers. Appropriately tailored efforts are critical to protect consumers from deception and other harm. We urge the Committee to support the Federal Communications Commission's unprecedented work to bring enforcement actions against illegal actors, while facilitating the ability of legitimate businesses to place valued and important calls to their customers using modern communications technologies.

Under its existing authority, the Commission has taken significant enforcement actions against illegal actors. For example, the Commission fined Adrian Abramovich $120 million for making nearly 100 million spoofed calls over three months,[1] fined telemarketer Philip Roesel and his companies more than $82 million for illegal caller ID spoofing,[2] and proposed a more than $37.5 million fine against Affordable Enterprises of Arizona for making millions of illegally-spoofed telemarketing calls.[3] We support appropriate enforcement actions to mitigate the harm caused to consumers by fraudulent and scam calls.

However, consumers are also harmed when they do not receive time-sensitive calls and text messages from legitimate businesses. Fraud alerts, data breach notifications, reminders to renew prescriptions or schedule a visit to the doctor, notifications of power outages, and automobile recall notices are consumer-benefitting calls that must be placed immediately to be of value to the recipient. It is critical that these calls and text messages be completed. As the Committee moves forward with its efforts in this area, we ask that it clearly distinguish between illegal callers and legitimate businesses. To that end, we are concerned that the legislation under

[1] Fed. Commc'ns Comm'n, News Release, Robocall Scammer Faces $120 Million Proposed Fine for Massive Caller ID Spoofing Operation (June 22, 2017), https://docs.fcc.gov/public/attachments/DOC-345470A1.pdf.
[2] Fed. Commc'ns Comm'n, News Release, FCC Fines Robocaller $82 Million for Illegally-Spoofed Health Insurance Marketing Calls (Sept. 26, 2018), https://docs.fcc.gov/public/attachments/DOC-354284A1.pdf.
[3] Fed. Commc'ns Comm'n, News Release, FCC Proposes $37.5 Million Fine for Spoofed Marketing Calls Appearing to Come from Consumers (Sept. 26, 2018), https://docs.fcc.gov/public/attachments/DOC-354286A1.pdf.

consideration by the Subcommittee will have unintended consequences that could negatively impact consumers as well as the broader business community. For example, H.R. 946 (the "Stopping Bad Robocalls Act") goes far beyond the scope of addressing the illegal actors who make abusive automated calls. In its current form, the legislation would harm businesses and consumers by impeding legitimate calls that consumers actually need or want.

Furthermore, the business community is also concerned about the current lack of regulatory clarity regarding the Telephone Consumer Protection Act (TCPA). This statute was intended to target abusive telemarketing calls, and not "be a barrier to the normal, expected or desired communications between businesses and their customers."[4] However, uncertainty following a recent ruling by the D.C. Circuit Court of Appeals threatens the ability of legitimate callers to communicate with the consumers with whom they have a relationship.

Accordingly, we ask that you work with the Commission to provide clarity surrounding legitimate informational communications, while continuing your important work to impede truly abusive calls.

Sincerely,

ACA International
American Association of Healthcare Administrative Management
American Bankers Association
American Financial Services Association
Coalition of Higher Education Assistance Organizations
Credit Union National Association
Edison Electric Institute
Insights Association
National Association of Federally-Insured Credit Unions
National Restaurant Association
National Retail Federation
Professional Association for Customer Engagement
Student Loan Servicing Alliance
The Consumer Bankers Association
The Electronic Transactions Association
U.S. Chamber Institute for Legal Reform
U.S. Chamber of Commerce

cc: Members of the Subcommittee on Communications and Technology

[4] H.R. Rep. No. 102-317, at 17 (1991).

April 29, 2019

The Honorable Michael F. Doyle, Chairman
The Honorable Robert E. Latta, Ranking Member
Subcommittee on Communications and Technology
Committee on Energy and Commerce
United States House of Representatives
Washington, D.C. 20515

Dear Chairman Doyle and Ranking Member Latta:

Consumer Reports[1] thanks you for holding this hearing to explore the problem of unwanted robocalls. Robocalls continue to plague consumers, disrupting peace of mind, interrupting important time with family, and enabling scams to enter consumers' homes. Truecaller found in 2018 that consumers had lost nearly $9 billion to phone scams in a 12-month period.[2] And neighbor spoofing, in which a caller spoofs the first six digits of the caller ID, is a significant problem, impeding call-blocking services and tricking consumers into picking up the phone.[3]

A new Consumer Reports national survey released earlier this month found that 70 percent of consumers don't even pick up the phone anymore if they don't recognize the number, because their phones are so overrun with unwanted robocalls.[4]

Consumer Reports has been working for a number of years to strengthen consumer protections against unwanted and invasive robocalling. We are encouraged to see several bills introduced that will help achieve this goal.

---

[1] Consumer Reports is an independent, nonprofit member organization that works side by side with consumers for truth, transparency, choice, and fairness in the marketplace. Founded in 1936, Consumer Reports has the largest nonprofit educational and consumer product testing center in the world, and uses its dozens of labs, auto test center, and survey research center to rate thousands of products and services annually. CR's premier magazine Consumer Reports has more than 3.6 million subscribers, and the award-winning CR.org has 2.9 million paying members and more than 15 million unique visitors monthly, on average. We use our rigorous research, consumer insights, journalism, and policy expertise to inform purchase decisions, improve the products and services that businesses deliver, and drive effective legislation and regulation -- to create a fairer, safer, and healthier world.

[2] Kim Fai Kok, *Truecaller Insights Reveal: Estimated 24.9M Americans Lost $8.9B in Phone Scams as Rate of Spam Calls Jumps 22%* (Apr. 26, 2018), https://truecaller.blog/2018/04/26/truecaller-insights-usa-2018/.

[3] Fed. Commc'ns Comm'n, Caller ID Spoofing (last updated Mar. 4, 2019), https://www.fcc.gov/consumers/guides/spoofing-and-caller-id.

[4] https://www.consumerreports.org/robocalls/mad-about-robocalls/.

We strongly support H.R. 946, the Stopping Bad Robocalls Act. This legislation would make a number of important improvements, including: ensuring that the definition of "autodialer" clearly covers all technology used to make robocalls and robotexts; affirming a consumer's right to revoke consent in any reasonable manner; strengthening FCC enforcement authority against unlawful robocalling; and requiring phone companies to provide consumers with technology, at no charge, to identify and stop spoofed calls.[5]

We also strongly support H.R. 2298, the ROBOCOP Act, which would clarify that protections against robocalling also cover robo-texting, and would require phone companies to offer to consumers free tools to identify and block all unwanted robocalls and robo-texts.[6]

We also support H.R. 1421, the HANGUP Act, to remove the exemption added to the Telephone Consumer Protection Act in 2015 that allows robocalling without consent by private debt collectors when they are collecting debts under contract with the federal government.[7]

Consumers strongly support these reforms. In recent months, Consumer Reports has gathered nearly 200,000 signatures on our petition calling on the FCC to require phone companies to implement caller ID authentication as soon as possible. Consumer Reports assisted over 30,000 consumers in submitting comments to the FCC this summer, urging them to issue strong rules to protect consumers from unwanted robocalls. Recently, Consumer Reports has also helped consumers send over 260,000 messages to Congress, asking for strong anti-robocalls legislation.

We look forward to working with you to see these important consumer protections enacted into law.

Sincerely,

Maureen Mahoney
Policy Analyst
San Francisco, CA

George P. Slover
Senior Policy Counsel
Washington, DC

cc: Members, Subcommittee on Communications and Technology

---

[5] H.R. 946 (2019).
[6] H.R. 2298 (2019).
[7] H.R. 1421 (2019).

epic.org

Electronic Privacy Information Center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

April 29, 2019

The Honorable Michael F. Doyle, Chair
The Honorable Robert Latta, Ranking Member
U.S. House Committee on Energy and Commerce
Subcommittee on Communications and Technology
2125 Rayburn House Office Building
Washington, D.C. 20515

Dear Chairman Doyle and Ranking Member Latta:

We write to you regarding the upcoming hearing on "Legislating to Stop the Onslaught of Annoying Robocalls."[1] In EPIC's view, the FCC needs to do far more to protect consumers from robocalls.

EPIC is a public interest research center established in 1994 to focus public attention on emerging privacy and civil liberties issues.[2] For over twenty years, EPIC has worked to ensure that the FCC protects the privacy of American consumers.[3] We are now concerned that the Commission has abdicated one of its most important responsibilities to the American public. The FCC must do more to safeguard American consumers.

Americans are suffering from an epidemic of robocalls. In 2018 alone, it is estimated that 47.8 billion robocalls were made in the United States, an increase of more than 50% over the prior year.[4] The Federal Communications Commission is charged with enforcing the Telephone Consumer Protection Act ("TCPA"), the law that Congress passed in 1991 to prevent precisely this problem.[5]

---

[1] *Legislating to Stop the Onslaught of Annoying Robocalls*, 116th Cong. (2019), H. Comm. on Energy and Commerce, Subcomm. on Communications and Technology (April 30, 2019), https://energycommerce.house.gov/committee-activity/hearings/hearing-on-legislating-to-stop-the-onslaught-of-annoying-robocalls.
[2] *See* EPIC, *About EPIC*, https://epic.org/epic/about.html.
[3] *See EPIC, CPNI (Customer Proprietary Network Information)*, https://epic.org/privacy/cpni/#EPIC (outlining the history of EPIC's advocacy for consumer privacy rules at the FCC, including two successful campaigns for pro-consumer rule changes); EPIC, *US West v. FCC – The Privacy of Telephone Records*, https://epic.org/privacy/litigation/uswest/ (1997) (describing the efforts of EPIC and others to defend the FCC's customer proprietary network information ("CPNI") rules); *see also* EPIC *Amicus brief, NCTA v. FCC*, 555 F.3d 996 (D.C. Cir. 2009) (defending the FCC's CPNI privacy rules); Letter from EPIC to the U.S. House of Representatives Committee on Energy and Commerce on FCC Privacy Rules (June 13, 2016), https://epic.org/privacy/consumer/EPIC-FCC-Privacy-Rules.pdf.
[4] *Nearly 48 Billion Robocalls Made in 2018, According to YouMail Robocall Index*, PR Newswire (Jan. 23, 2019), https://www.prnewswire.com/news-releases/nearly-48-billion-robocalls-made-in-2018-according-to-youmail-robocall-index-300782638.html.
[5] 47 U.S.C. § 227.

The FCC knows of the scope of the problem.[6] But so far the Commission has been unable to stop or even reduce the flow of unwanted calls. And the Commission is simultaneously soliciting proposals from telemarketing industry groups to would weaken the TCPA rules that are supposed to protect consumers from nuisance calls.[7]

EPIC has repeatedly warned the Commission about the need to strengthen, not weaken, privacy protections in the TCPA rules. For example, in response to the FCC's notice in May 2018, EPIC filed detailed comments explaining why the Commission should not modify the regulations to exempt millions of unwanted calls and leave consumers without legal rights.[8] The Commission has twice sought comment on the question of "what constitutes an 'automatic telephone dialing system'" under the TCPA.[9] This definition is central to the entire structure of the law, and if the Commission improperly narrows the definition, many consumers will be left without legal protection from unwanted calls. The FCC's willingness to eliminate consumer protections when we are experiencing an unprecedented increase in robocalls contradicts the agency's mission and would further the TCPA's deterrent effect.

We ask that this letter be submitted into the hearing record. EPIC looks forward to working with the Subcommittee on this issue.

Sincerely,

/s/ Marc Rotenberg
Marc Rotenberg
EPIC President

/s/ Caitriona Fitzgerald
Caitriona Fitzgerald
EPIC Policy Director

/s/ Alan Butler
Alan Butler
EPIC Senior Counsel

---

[6] Fed. Commc'ns Comm'n, *The FCC's Push to Combat Robocalls & Spoofing* (2019), https://www.fcc.gov/about-fcc/fcc-initiatives/fccs-push-combat-robocalls-spoofing.

[7] Public Notice, Fed. Commc'ns Comm'n, *Consumer and Governmental Affairs Bureau Seeks Comment on Interpretation of the Telephone Consumer Protection Act in Light of the D.C. Circuit's ACA International Decision*, 33 FCC Rcd. 4864 (May 14, 2018), https://www.fcc.gov/document/cgb-seeks-comment-tcpa-light-dc-circuit-decision-aca-intl.

[8] Comments of EPIC to the Fed. Commc'ns Comm'n, *Interpretation of the Telephone Consumer Protection Act in Light of the D.C. Circuit's ACA International Decision*, DA-18-493, CG 02-278, CG 18-152 (June 13, 2018), https://epic.org/apa/comments/EPIC-FCC-TCPA-June2018.pdf; Reply Comments of EPIC to the Fed. Commc'ns Comm'n, *Interpretation of the Telephone Consumer Protection Act in Light of the D.C. Circuit's ACA International Decision*, DA-18-493, CG 02-278, CG 18-152 (June 28, 2018), https://epic.org/apa/comments/EPIC-FCC-TCPA-ReplyComments-June2018.pdf.

[9] Public Notice, 33 FCC Rcd. 4864, *supra*; Public Notice, Fed. Commc'ns Comm'n, *Consumer and Governmental Affairs Bureau Seeks Comment on Interpretation of the Telephone Consumer Protection Act in Light of the Ninth Circuit's Marks v. Crunch San Diego, LLC Decision*, DA-18-493, CG 02-278, CG 18-152 (Oct. 3, 2018)

3138 10th Street North
Arlington, VA 22201-2149
703.522.4770 | 800.336.4644
f: 703.524.1082
nafcu@nafcu.org | nafcu.org

National Association of Federally-Insured Credit Unions

April 29, 2019

The Honorable Michael Doyle
Chairman
Subcommittee on Communications & Technology
Committee on Energy and Commerce
U.S. House of Representatives
Washington, D.C. 20515

The Honorable Robert Latta
Ranking Member
Subcommittee on Communications & Technology
Committee on Energy and Commerce
U.S. House of Representatives
Washington, D.C. 20515

Re: Tomorrow's Hearing on "Legislating to Stop the Onslaught of Annoying Robocalls"

Dear Chairman Doyle and Ranking Member Latta:

I write to you today on behalf of the National Association of Federally-Insured Credit Unions (NAFCU) in conjunction with tomorrow's hearing entitled "Legislating to Stop the Onslaught of Annoying Robocalls." NAFCU advocates for all federally-insured not-for-profit credit unions that, in turn, serve over 116 million consumers with personal and small business financial service products. NAFCU and our members appreciate the Subcommittee tackling the scourge of unwanted, illegal robocalls, but we would caution the Subcommittee to ensure that these well-intentioned efforts do not impede legitimate calls from credit unions made using an automatic telephone dialing system (ATDS or autodialer).

NAFCU supports your goal to thwart unlawful actors who seek to defraud or commit other unlawful acts against consumers. We believe that appropriately tailored legislative efforts are critical to protect consumers from deception and other harm. NAFCU supports the Federal Communications Commission's (FCC) unprecedented work to bring enforcement actions against illegal actors. However, we continue to engage the FCC to seek clarity on the ability of credit unions to place valued and important calls to their customers using modern communications technologies.

In particular, NAFCU has concerns with the FCC's continuing work on defining an "autodialer" under the *Telephone Consumer Protection Act* (TCPA). Since the FCC issued its problematic 2015 Declaratory Ruling and Order (2015 Order), the risk of facing a costly lawsuit over inadvertent TCPA violations has kept many credit unions from freely communicating with their members. The March 2018 *ACA International v. FCC* decision invalidated the 2015 Order's overly expansive definition of "autodialer" and the FCC's approach to liability for calls to reassigned numbers under the TCPA. Following that decision, courts have taken a variety of approaches in determining what qualifies as an "autodialer" – leading to a maze of judicial interpretations of Congress's intent and meaning in passing the TCPA.

NAFCU supports a broad definition of "autodialer" that only includes equipment that uses a random or sequential number generator to store or produce numbers and dial those numbers without human intervention. As such, NAFCU is concerned that some of the legislation in question during this hearing poses a threat to credit unions' ability to make legitimate communications to their members. For example, H.R. 946, the *Stopping Bad Robocalls Act*, includes a definition of "robocall" that greatly expands the TCPA's definition of "autodialer" and would effectively sweep in and place limitations on a broader set of communications and call dialing equipment than previously contemplated. NAFCU cannot support legislation that conflates illegal robocalls with autodialed calls made by good faith callers for legitimate purposes.

We appreciate the Subcommittee's continued oversight of the FCC and examination of this issue and would urge the Subcommittee to modernize the TCPA to combat illegal robocalls, while also protecting credit unions' ability to freely communicate with their members on important issues related to their existing accounts. NAFCU encourages the Subcommittee to consider other reforms to help resolve uncertainties with TCPA compliance, such as permitting callers to establish a reasonable opt-out method for revoking their consent to be contacted. As the Subcommittee reviews the bills before this hearing tomorrow, we would urge you to ensure that efforts to stop illegal robocalls do not negatively impact the ability of credit unions to contact their members for legitimate business purposes.

On behalf of our nation's credit unions and their more than 116 million members, we thank you for your attention to this important matter. Should you have any questions or require any additional information please contact me or Alex Gleason, NAFCU's Associate Director of Legislative Affairs, at 703-842-2237 or agleason@nafcu.org.

Sincerely,

Brad Thaler
Vice President of Legislative Affairs

cc: Members of the Subcommittee on Communications & Technology

April 29, 2019

The Honorable Michael F. Doyle
Chairman
Committee on Energy and Commerce
Subcommittee on Communications & Technology
U.S. House of Representatives
Washington, DC 20515

The Honorable Robert Latta
Ranking Member
Committee on Energy and Commerce
Subcommittee on Communications & Technology
U.S. House of Representatives
Washington, DC 20515

Dear Chairman Doyle and Ranking Member Latta:

On behalf of ACA International, I am writing regarding the hearing, ""Legislating to Stop the Onslaught of Annoying Robocalls," in the Energy and Commerce Subcommittee on Communications & Technology. ACA International is the leading trade association for credit and collection professionals representing approximately 2,500 members, including credit grantors, third-party collection agencies, asset buyers, attorneys, and vendor affiliates in an industry that employs more than 230,000 employees worldwide.

ACA members are also consumers, and like many consumers, greatly dislike fraudulent and illegal robocalls. Accordingly, we appreciate that the Subcommittee is working to stop those making such abusive calls. We also appreciate the Federal Communications Commission's (FCC) efforts to combat illegal robocalls through enforcement actions, including levying millions of dollars of fines against bad actors. These efforts are certainly worthwhile and deserve the serious attention they have been given by the FCC and Congress. However, since scammers by their very nature are operating outside the bounds of the law and have no intention to follow the law as it is now or in the future, very often they do not pay the fines levied against them for bad behavior as recently noted in the *Wall Street Journal*.[1] On the other hand, unclear requirements under the Telephone Consumer Protection Act (TCPA) have cost legitimate businesses seeking to follow the law millions of dollars in class action settlements, even though the lion's share of those funds are often given to attorneys not consumers.[2]

[1] Krouse, Sarah, *The FCC Has Fined Robocallers $208 Million. It's Collected $6,790*, available at https://www.wsj.com/articles/the-fcc-has-fined-robocallers-208-million-its-collected-6-790-11553770803 (March 28, 2019).
[2] U.S. Chamber Institute for Legal Reform, *TCPA Lawsuits are HOW Expensive??*, available at https://www.instituteforlegalreform.com/resource/tcpa-lawsuits-are-how-expensive. "The average cost of a TCPA settlement in 2018 was $6,600,000."

ASSOCIATION HEADQUARTERS
4040 WEST 70TH STREET 55435
P.O. BOX 390106, MINNEAPOLIS, MN 55439-0106
TEL (952) 926-6547 FAX (952) 926-1624

FEDERAL GOVERNMENT AFFAIRS OFFICE
509 2ND STREET NE, WASHINGTON, D.C. 20002
TEL (202) 547-2670
FAX (202) 547-2671

ACA@ACAINTERNATIONAL.ORG WWW.ACAINTERNATIONAL.ORG

The accounts receivable management industry is a highly regulated industry complying with applicable federal and state laws and regulations regarding debt collection, as well as ethical standards and guidelines established by ACA. The collection activities of ACA members are regulated at the state level and by the Bureau of Consumer Financial Protection (CFPB or Bureau), which supervises and examines Large Market Participants in the industry. Furthermore, the industry is awaiting federal rules under the Fair Debt Collection Practices Act, which are expected to provide guidance about communication with consumers in the next few weeks. ACA members contact consumers exclusively for non-telemarketing reasons to facilitate the recovery of payment for services that have already been rendered, goods that have already been received, or loans that have already been provided. The use of modern technology is critical for the ability to contact consumers in a timely and efficient matter, and often the sooner in the collection process that a consumer is put on notice of a debt, the better off they are.

The Stopping Bad Robocalls Act Threatens Legitimate Businesses and Misses the Mark in Targeting Bad Actors

Unfortunately, through certain sweeping efforts to stop bad actors some policymakers are either intentionally or unintentionally impeding legitimate calls that include important information such as account updates, school closings, loss of utilities, and other exigent information for consumer. As a whole, H.R. 946, the Stopping Bad Robocalls Act, misses the mark in targeting those harming consumers. Instead, the outcome of the legislation will have a negative impact on consumers' ability to receive information they need from legitimate businesses. Specifically, the overly broad characterization of what is considered a "robocall" and the proposed expanded definition of what is considered an autodialer fly in the face of what court decisions have already reasoned to be arbitrary and capricious.[3] Under the Stopping Bad Robocalls Act, it is possible that nearly any call other than one coming from a rotary phone could be considered a "robocall." In looking at consumers' preferred methods of communications and the advances in today's technology that have made consumers' lives better by being more informed about pressing matters in a more timely way, returning to an error of only allowing communications by outdated technology is clearly not beneficial. Unfortunately, the Stopping Bad Robocalls Act would create a dangerous environment obstructing dialogue about important matters and set consumers back decades in their ability to be informed.

Consumers often need the information that ACA members provide to maintain their financial health. This open communication can lead to the most favorable outcome for consumers. We appreciate the House Financial Services Committee's recent recognition of this concept during the federal government shutdown in a letter that acknowledged, "...once negative information is reported to consumer reporting agencies, affected employees are likely to see a reduction in their credit scores. This may limit their ability to access credit or result in higher interest rates and more costly terms on credit in the future. Prudent workout arrangements that are consistent with safe-and-sound lending practices are generally in the long-term best interest of the financial

[3] *ACA Int'l, et al.* v. *FCC*, 885 F.3d 6 (D.C. Cir. 2018) (mandate issued May 8, 2018) (affirming in part and vacating in part Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, CG Docket No. 02-278, WC Docket No. 07-1 Rcd 7961 (2015).

institution, the borrower, and the economy."[4] The ability to communicate with consumers is pertinent to have these critical discussions.

This lack of clarity created by the Stopping Bad Robocalls Act would also have a disproportionately harmful impact on small businesses and smaller financial institutions, which already have a difficult time navigating how to comply with onerous requirements for what is considered an autodialer.[5] This is compounded by the opaque ways that consent, already provided, could be revoked under the Stopping Bad Robocalls Act creating confusion for both consumers and businesses. Furthermore, it is critical to ensure that small businesses and all callers have a seat at the table to formulate any "call authentication" mechanisms, including those discussed in the legislation, to ensure that legitimate callers are not faced with unreasonable or unworkable burdens in trying to make critical informational calls.

Also, under the legislation the term "called party" would be defined as "with respect to a call, the current subscriber of the telephone number to which the call is made, determined at the time when the call is made." ACA has sought clarity on this same issue from the FCC by urging it to interpret called party as the party that the caller reasonably expected to reach as the intended recipient. This makes the most sense to be able to have reasonable reliance on the prior express consent given for the intended recipient. The FCC now has the opportunity to amend past flawed analysis about this. However, the provisions in the Stopping Bad Robocalls Act are a step in the wrong direction from doing that.

Congress Should Support Clarity Surrounding the TCPA

We ask that the Subcommittee, in addition to considering the problems created by illegal actors making robocalls, also consider the importance of legitimate business calls currently impeded by onerous TCPA requirements. Specifically, ACA would like the Subcommittee to consider these points.

- TCPA interpretations remain onerous and create unclear compliance expectations that leave businesses vulnerable to frivolous class action litigation. The FCC must act to clarify its interpretations of the TCPA as directed by the D.C. Circuit Court of Appeals (D.C. Circuit) after the decision in *ACA Int'l v. FCC*[6];
- New call blocking and labeling technologies are unfairly impeding calls from credit and collection professionals and other legitimate businesses, in some instances in deceptive

[4] Letter from Chairwoman Maxine Waters about the federal government shutdown, available at https://financialservices.house.gov/uploadedfiles/shutdown_letter_to_industry_011819.pdf (January 18, 2019).
[5] Ex parte Notice of SBA Office of Advocacy, Consumer and Government Affairs Bureau Seeks Comment on Interpretation of the Telephone Consumer Protection Act in Light of the D.C. Circuit's ACA International Decision, CG Docket Nos. 18-152, 02-278. "The SBA Office of Advocacy addressed the confusion surrounding the TCPA as it pertains not only to consumers but small business owners. The SBA Office of Advocacy stated, 'In an environment where fifty to seventy [percent] of a business' customers might only be reachable by mobile phone, it is important that the FCC move quickly to establish clear guidance to small business compliance without depriving customers of required or desired communications.'"
[6] *ACA Int'l, et al.* v. *FCC*, 885 F.3d 6(D.C. Cir. 2018) (mandate issued May 8, 2018) (affirming in part and vacating in part Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, CG Docket No. 02-278, WC Docket No. 07-1 Rcd 7961 (2015).

ways, or ways that engage in slanderous labeling of legitimate calls (*See* Attachment); and

- Several regulators including the U.S. Department of the Treasury (Treasury), the Small Business Administration (SBA) Office of Advocacy; and the CFPB have recognized the importance of legitimate businesses having the ability to communicate with consumers.

Regulators Have Stressed the Need for Clarity Concerning the TCPA

As the Treasury recently acknowledged in its report, *A Financial System That Creates Economic Opportunities Nonbank Financials, Fintech, and Innovation*, "Debt collectors and debt buyers play an important role in minimizing losses in consumer credit markets, thereby allowing for increased availability of and lower priced credit to consumers."[7] In addition to the overall economic benefits the industry provides, the Treasury also addresses how the ability to communicate with consumers is harmed by the TCPA. In the report, the Treasury states, "Current implementation of the TCPA constrains the ability of financial services firms to use digital communication channels to communicate with their customers despite consumers' increasing reliance on text messaging and email communications through their mobile devices."

Similarly, the SBA Office of Advocacy addressed the confusion surrounding the TCPA as it pertains not only to consumers but small-business owners. The SBA Office of Advocacy stated, "In an environment where fifty to seventy [percent] of a business' customers might only be reachable by mobile phone, it is important that the FCC move quickly to establish clear guidance to small business compliance without depriving customers of required or desired communications."[8] Furthermore, the CFPB noted in a letter to the FCC that, "Consumers benefit from communications with consumer financial products providers in many contexts, including receiving offers of goods and services and notifications about their accounts. Recent years have seen rapid increases in the use of smart phones, text messages, email, social media, and other new or newer methods of communication. With the advent and deployment of these communication technologies, it is important to review how statutes and regulations apply to them."[9]

While illegal actors certainly deserve scrutiny from Congress and the FCC, as highlighted, multiple regulatory agencies have also recognized there are significant benefits to consumers when they can communicate with legitimate businesses and institutions. The D.C. Circuit Court, as previously noted, struck down the FCC's previous interpretation of the TCPA, finding parts of it arbitrary and capricious including the broad definition of autodialer. Unfortunately, the Stopping Bad Robocalls Act is a step backwards in providing the additional clarity the courts have asked the FCC to provide. It is not helpful in clarifying a severely outdated statute enacted

---

[7] U.S. Department of Treasury, *A Financial System That Creates Economic Opportunities Nonbank Financials, Fintech, and Innovation* (July 2018), available at https://home.treasury.gov/sites/default/files/2018-07/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financi....pdf.

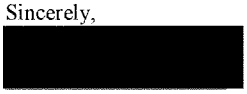
[8] Ex parte Notice of SBA Office of Advocacy, Consumer and Government Affairs Bureau Seeks Comment on Interpretation of the Telephone Consumer Protection Act in Light of the D.C. Circuit's ACA International Decision, CG Docket Nos. 18-152, 02-278.

[9] Comments of the Bureau of Consumer Financial Protection, In the Matter of Rules and Regulations Implementing the Telephone Consumer Protection Act and CG Docket No. 02-278 Interpretations in Light of the D.C. Circuits CG Docket No. 18-152 ACA International Decision (June 13, 2018).

in 1991 that has not kept up with modern technology and consumers' preferences or targeting fraudulent actors making robocalls. Instead, it will make it harder for legitimate businesses to contact consumers, and for those consumers to learn about information they need to preserve their ability to access credit, health services, and a large variety of other exigent information.

Thank you for holding the hearing and your attention to these important matters.

Sincerely,



Mark Neeb
Chief Executive Officer

The Impact of Call-blocking and Labeling Technologies on the Accounts Receivable Industry

ACA INTERNATIONAL
The Association of Credit and Collection Professionals

As consumer "robocall" complaints continue to escalate, regulators have turned their focus to technological solutions to stop illegal calls from reaching consumers. After being given the green light by the Federal Communications Commission, carriers and other providers have begun offering consumers various call-blocking tools. However, legitimate businesses, including debt collectors, are discovering their calls are showing up on consumer phones as "suspected scam" or are even being blocked outright.

The misclassification of legitimate business calls as a scam and the blocking of such calls is a serious issue that threatens the fundamental ability of debt collectors to communicate with consumers to share important account information. This has prompted complaints about legitimate call attempts against the industry and causes reputational harm when calls are labeled with confusing and potentially slanderous labels.

In a recent survey, ACA members were asked to indicate whether their calls were being blocked or potentially mislabeled. The majority of respondents indicated that they were experiencing call-blocking (78%) or having their calls mislabeled (74%) (see Figures 1 and 2). Additionally, 62% of respondents reported that they were seeing a decrease in right-party contacts (Figure 3).

Figure 1. Percent of Respondents indicating that their Calls are being Blocked.

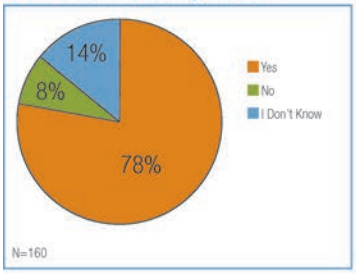


Figure 2. Percent of Respondents indicating that their Calls are being Mistakenly Labeled as "Scam", "Fraud", or Other Improper Label.

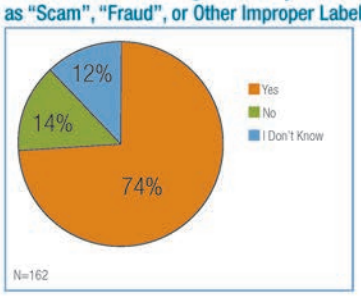
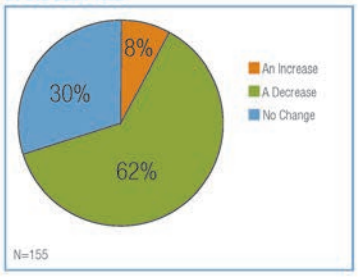


Figure 3. Percent of Respondents Indicating a Change in Right-Party Contacts in the Last Year.



» continues on reverse

© 2018 ACA International. All rights reserved.

ACA International asked our members how these technologies were impacting their business and consumers. Here is what they had to say:

How are ACA members discovering that their calls are being blocked or Labeled?

- The consumers are telling us that our calls are labeled as Spam or Scam which creates mistrust of our legitimate reason for calling.
- Our consumers advised of it. When speaking with a consumer they ask "why does your number show as 'spam'"?
- A consumer called us to advise us that our missed call was labeled as possible scam.
- Consumers advised us that they saw it on their phone and suspected that we were a scam. They would refuse to verify their information so we could discuss their account.
- Consumer informed that it showed up on their phone as "Possible Scam."

How does this issue impact ACA members' relationships with consumers?

- This has a huge impact because the majority of phone numbers are with cell phone providers that are blocking our calls. Consumers don't have the ability to resolve their account until it is too late to avoid debts being reported to their credit report.
- The consumers we're attempting to reach do not want to answer because their phone says we're a scam. Many consumers now have call blocker apps that we've erroneously been added to because they think our company is a scam. What if we report something to someone's credit and it prevents them from purchasing a home, car, security clearance, etc? That's not fair to the consumers.
- The consumers, as well as our agency, have been impacted. Some have shared they wished they had taken the call but honestly thought it was spam. As a result, the account went unresolved which did not help the consumer.
- Consumers are less likely to answer their phone, they think that our business is not legitimate, and has caused complaints to regulators and our clients. Consumers are then not resolving their accounts which continue to potentially impact them negatively.
- Consumers are less receptive to our collectors when they get them on the phone and less likely to verify their information. We already have to sound shady when we ask debtors to verify their SSN or DOB. If the caller ID says it is a scam then the person on the line is asking about your SSN no person in their right mind would verify.

How does this issue impact the ability of ACA members to conduct business?

- Our call/contact ratio has declined 40% against the call/contact ratio in prior years and has decreased our client's recovery of unresolved accounts.
- We are unable to contact consumers that legitimately want to talk to us and find solutions to their accounts.
- Few contacts will result in lower recoveries and more disputes. It will also result in consumers not knowing about their debt until after we've reported it to the CRAs and by then, whatever impact we may have had to their credit is done.
- Major impact and consumers are less likely to answer the call. It also impacts our credibility as a business with a legitimate business matter.
- Telephone calls are an essential process for collection agencies. It's what we do. The impact is life or death of the company.

What does ACA want lawmakers to do about this?

Consider developing protocols and/or a regulatory framework directed at call blocking and labeling companies to require them to differentiate between legal informational calls and illegal robocallers.

© 2018 ACA International. All rights reserved.

DR. JEFFERSON VAN DREW
2ND DISTRICT OF NEW JERSEY

CONGRESS OF THE UNITED STATES
HOUSE OF REPRESENTATIVES
WASHINGTON, D.C. 20515

HOUSE AGRICULTURE COMMITTEE
SUBCOMMITTEE ON COMMODITY EXCHANGES, ENERGY AND CREDIT
SUBCOMMITTEE ON BIOTECHNOLOGY, HORTICULTURE AND RESEARCH
SUBCOMMITTEE ON NUTRITION, OVERSIGHT AND DEPARTMENT OPERATIONS
SUBCOMMITTEE ON GENERAL FARM COMMODITIES AND RISK MANAGEMENT
HOUSE NATURAL RESOURCES COMMITTEE
SUBCOMMITTEE ON WATER, OCEANS AND WILDLIFE

CO-CHAIR OF THE BLUE DOG COALITION
TASKFORCE ON NATIONAL SECURITY

April 30, 2019

Chairman Doyle, Ranking Member Latta, and members of the Communications and Technology Subcommittee, I thank you for including my bill, H.R. 1575, "The Robocall Enforcement Enhancement Act of 2019", in today's legislative hearing entitled, "Legislating to Stop the Onslaught of Annoying Robocalls".

I appreciate the opportunity you have given me today to speak about the annoying and incessant telemarketing and robocalls that we all, and millions across America, receive daily. Telemarketing scams are at an all time high, and the use of robocalls and spoofing practices in those scams has been an important key to their success. The Robocall Enforcement Enhancement Act of 2019:

- Authorizes the FCC to pursue cases against rule violations without first issuing a citation;
- Increases the stature of limitations for the FCC to pursue spoofing violations from two years to three years; and
- Increases the statute of limitations for the FCC to pursue robocall violations from one year to three years.

As a New Jersey State Senator, I sponsored the original Do Not Call list for the state and fought to strengthen that list to limit the ability of robocallers to annoy and prey upon our citizens. Data shows that New Jersey residents reported 321,393 robocall complaints last year alone - more than any other state in the nation.

Robocall scams are at an all-time high and getting worse. One report estimates that the number of spam calls will grow from 30 percent of all phone calls in 2018 to 42 percent in 2019. In 2017 alone, the Federal Trade Commission received more than 4.5 million robocall complaints, an increase of over a million calls from the year before. Many of these scams take advantage of senior citizens and other vulnerable populations, and it is time we protect consumers by ensuring those who violate the law are prosecuted to the fullest extent of the law.

I appreciate the subcommittee's attention to this timely problem.

Sincerely,

Jeff Van Drew
U.S. Representative
New Jersey – District 2

Attachment—Additional Questions for the Record

Subcommittee on Communications and Technology
Hearing on
"Legislating to Stop the Onslaught of Annoying Robocalls"
April 30, 2019

Mr. Patrick Halley, Senior Vice President, Advocacy and Regulatory Affairs, USTelecom – The Broadband Association

The Honorable David Loebsack (D-IA)

1. **What specific work is currently being done to overcome the limitations of copper networks for the implementation of anti-robocall technology like STIR/ SHAKEN?**

Response: Although the SHAKEN/STIR standards are designed for implementation across Internet Protocol (IP) networks, industry is working on solutions to overcome the limitations to deployment on traditional time division multiplexing (TDM) networks (*i.e.*, copper networks). For example, the Network Working Group of the Internet Engineering Task Force (IETF) in March, 2019, published an Internet Draft working paper entitled *STIR Out-of-Band Architecture and Use Cases* ("*IETF Paper*") which addresses potential approaches for deployment of SHAKEN/STIR capabilities on traditional TDM networks.[1]

The *IETF Paper* discusses certain limitations of TDM networks for deployment of SHAKEN/STIR. It notes for example, that even if fields for sending authentication information could be found in traditional public switched telephone networks (PSTN) signaling, the "legacy elements would strip the signatures from those fields," or "might damage them to the point where they cannot be verified."[2] However, the *IETF Paper* observes that while the core network of the PSTN remains fixed, "the endpoints of the telephone network are becoming increasingly programmable and sophisticated."[3]

It states that TDM networks are "shrinking, and increasingly being replaced" by various classes of "intelligent devices" such as IP Private Branch Exchanges (PBXs) and terminal adapters, all of which provide both Internet access and access to the PSTN. Additionally, the *IETF Paper* notes that various kinds of gateways "increasingly front for deployments of legacy PBX and

---

[1] *See* IETF Network Working Group, Internet Draft, STIR Out-of-Band Architecture and Use Cases (March 11, 2019) (available at: https://tools.ietf.org/html/draft-ietf-stir-oob-04#section-1) (visited June 21, 2019) (*IETF Paper*).

[2] *IETF Paper*, p. 3.

[3] *Id.*

PSTN switches."[4] It concludes that all of these factors "provides a potential avenue for building an authentication system that implements stronger identity while leaving PSTN systems intact."[5] The *IETF Paper* then discusses a "high-level architecture" for overcoming TDM limitations in certain use cases.[6]

As the IETF proceeds with its important work, and as networks continue their evolution from TDM to IP networks, there are currently solutions available in the marketplace that can address this issue on an interim basis. For example, TNS provides its Call Authentication Hub for SHAKEN/STIR that enables Tier 2 and Tier 3 carriers to deploy SHAKEN/STIR capabilities and can provide a solution for TDM carriers using out-of-band signaling.[7] Some industry stakeholders have also identified a variety of ways that carriers with traditional TDM trunks can implement STIR/SHAKEN that are consistent with the findings in the *IETF Paper*.[8] For example, a STIR/SHAKEN-aware gateway can be put in front of legacy infrastructure that will enable calls to show up as being valid signed calls at their destination. In addition, if there are endpoints or intermediaries in the legacy TDM infrastructure that can access the Internet, there can be an implementation of an out-of-band infrastructure for STIR/SHAKEN. Finally, an upstream carrier with an IP gateway can potentially sign calls on behalf of the carrier with traditional TDM trunks.

2. What do you estimate is the percentage of calls that are not pure, end-to-end IP?

Response: As discussed in response to the previous question, industry is working on solutions to overcome the limitations to deployment of STIR/SHAKEN on TDM networks, and interim solutions are available in the marketplace. While we do not know with precision the percentage of calls that are pure end-to-end IP, our best approximation is about half of calls are end-to-end IP today, with some margin of error in either direction. However this percentage is shrinking every day as carriers upgrade their infrastructure.

We are unaware of public data directly addressing the question. There is also some technical uncertainty regarding the extent to which a given call that originates and terminates at IP end-points remains on an IP path for the entirety of the call. Nonetheless, we can assume that this is the case for the purpose of a crude estimation.

---

[4] *Id.*

[5] *Id.*

[6] *IETF Paper*, pp. 11 – 15.

[7] *See*, TNS, *Ex Parte* Presentation to the FCC, GC Docket No. 17-59 and WC Docket No. 17-97 (filed May 28, 2019) (available at: https://ecfsapi.fcc.gov/file/10528829902187/TNS_FCC_Presentation_052319.pdf) (visited June 21, 2019) at p. 11 (discussing TNS Call Guardian Authentication Hub, which provides a pre-STIR/SHAKEN out of band capability for TDM carriers).

[8] *See*, Neustar website, *STIR/SHAKEN Q&A: Restoring Trust in Calls* (available at: https://www.home.neustar/resources/faqs/stir-shaken-q-and-a) (visited June 21, 2019).

According to 2017 Federal Communications Commission (FCC) data,[9] there were approximately 455 million business and residential end-user voice connections consisting of 65 million interconnected VoIP wired lines (14 percent), 55 million switched wired lines (12 percent), and 335 million wireless voice subscribers (74 percent). Assuming approximately four-fifths of wireless subscribers use IP-based technology that bypasses the TDM network, such as Voice over LTE,[10] we approximate that nearly three-quarters (73 percent) of end-user connections are IP and nearly one-quarter (27 percent) are switched. Based on highly simplified probabilities, we estimate that a little more than half of all calls (approximately 55 percent) are IP-to-IP, with the remainder originating, terminating, or both, on a switched network. However, these are merely estimates based on statistical probabilities, not actual call records.

---

[9] *See* FCC, Voice Telephone Services: Status as of June 30, 2017 (November 2018) at Table 1 (VTS). This analysis disregards non-interconnected, over-the-top communications.

[10] *See* Ericsson, Mobility Report (November 2018) at 13, available at https://www.ericsson.com/en/mobility-report/reports/november-2018 (visited June 21, 2019) (stating that 87 percent of North American wireless subscriptions are LTE). For our purposes, we assume a lower percentage of calls are LTE to account for potential non-LTE devices and usage, such as non-subscription devices that do not use LTE service (e.g., some prepaid phones) and LTE-capable devices roaming on non-LTE networks.

○