Diversified Reporting Services, Inc.
RPTS CARR
HIF155020

HEARING ON STOPPING ILLEGAL ROBOCALLS AND ROBOTEXTS:
PROGRESS, CHALLENGES, AND NEXT STEPS
WEDNESDAY, JUNE 4, 2025
House of Representatives,
Subcommittee on Oversight and Investigations,
Committee on Energy and Commerce,
Washington, D.C.

The Subcommittee met, pursuant to notice, at 10:15 a.m., in Room 2322, Rayburn House Office Building, Hon. Gary Palmer [chairman of the subcommittee] presiding.

Present: Representatives Palmer, Balderson, Griffith, Dunn, Crenshaw, Weber, Allen, Fulcher, Rulli, Guthrie [ex officio]; Clarke, DeGette, Tonko, Trahan, Fletcher, Ocasio-Cortez, Mullin, and Pallone [ex officio].

Also present: Representatives Joyce and Pfluger.

Staff present: Ansley Boylan, Director of Operations; Jessica Donlon, General Counsel; Sydney Greene, Director of

Finance and Logistics; Brittany Havens, Chief Counsel; Megan Jackson, Staff Director; Sophie Khanahmadi, Deputy Staff Director; Alex Khlopin, Clerk; John Lin, Senior Counsel; Sarah Meier, Counsel and Parliamentarian; Joel Miller, Chief Counsel; Chris Sarley, Member Services/Stakeholder Director; Joanne Thomas, Counsel; Matt VanHyfte, Communications Director; Aurora Ellis, Minority Law Clerk; Austin Flack, Minority Professional Staff Member; Waverly Gordon, Minority Deputy Staff Director and General Counsel; Tiffany Guarascio, Minority Staff Director; Will McAuliffe, Minority Chief Counsel, OI; Constance O'Connor, Minority Senior Counsel; Christina Parisi, Minority Professional Staff Member; Harry Samuels, Minority Counsel; and Caroline Wood, Minority Research Analyst.

*Mr. Palmer. Good morning, and welcome to today's hearing entitled Stopping Illegal Robocalls and Robotexts: Progress, Challenges, and Next Steps.

All of us have personal experiences with unwanted robocalls and robotexts. Some are merely annoying, but others have devastating consequences. For example, in March, the FCC warned consumers about scam robocalls targeting older Americans, and the Department of Justice announced that it charged 25 individuals for participating in the same scam that defrauded Americans out of more than $21 million in more than 40 states. The scammers made phone calls pretending to be an individual's grandchild who needed money for bail after being arrested, or pretended to be the grandchild's attorney and were told that they could not speak to anyone about the arrest. This is one of the many heartbreaking examples of scams perpetrated on Americans by illegal robocallers and bad actors.

According to recent estimates, in April of 2025, nearly 2,000 robocalls were placed to U.S. consumers every second. Spam and scam calls make consumers feel threatened, fearful, and distrustful of legitimate calls. As more and more Americans ignore calls from unknown numbers, they miss important calls. Moreover, fraud perpetrated against Americans by illegal robocalls costs an average of $25 billion annually, primarily affecting those who cannot afford such losses.

We are also seeing a lot of unwanted and scam robotexts and AI-generated phone calls and text messages, including voice clones and deepfakes. According to the FCC, consumer complaints about unwanted text messages increased 500 fold between 2015 and 2022. Americans are frustrated and understandably so.

In 2019, the bipartisan Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence, or TRACED Act, was enacted to help reduce the flood of illegal robocalls. The TRACED Act allowed the FCC and law enforcement to impose stricter penalties for intentional violations of the Telephone Consumer Protection Act, or TCPA, improved adoption of technical solutions like STIR and SHAKEN call authentication framework, and established a federal interagency working group to combat illegal robocalls. As a result, U.S. telecommunications carriers have made progress implementing STIR/SHAKEN into their networks.

This framework authenticates that phone calls are coming from legitimate phone numbers, which helps reduce the number of spoofed and illegal robocalls. Generally, to operate within the U.S., voice service providers must now implement robocall mitigation programs and file these plans in their STIR/SHAKEN compliance certifications in the robocall mitigation database overseen by the FCC. Moreover, in July

2020, the FCC recognized the USTelecom Industry Traceback Group as the single registered consortium to conduct private led traceback efforts that identified the source of an illegal robocall. The FCC has also taken measures to address the growing burden of unwanted and scam robotexts and abused AI technologies.

Specifically, in March 2023, the agency adopted regulations targeting scam robotexts. In addition, industry actors have partnered with federal agencies to launch new programs such as robotext tracing. Lastly, in August, the FCC proposed rules to protect consumers from AI-generated robocalls and robotexts.

These are steps in the right direction, and I applaud the coordination we have seen thus far. While the TCPA has provided many useful tools, the TCPA's private right of action has given rise to class action lawsuits focused on minor infractions rather than the bad actors responsible for placing illegal robocalls, and it has not reduced the number of illegal robocalls or improved consumer protection.

In addition, STIR/SHAKEN implementation among smaller carriers has been delayed, and bad actors have exploited these providers' reliance on legacy infrastructure. Moreover, a majority of illegal robocalls and robotexts originate overseas, making them hard to trace. Because these bad actors are outside the jurisdiction of U.S. law enforcement, they are challenging to combat.

Finally, the FCC must grapple with emerging technologies and navigate the best way to create appropriate guard rails for these technologies, while simultaneously continuing to support innovation. We will always have robocalls and robotexts because not all of them are illegal. Many are used for legitimate purposes by U.S. businesses and public entities. But we must continue finding ways to combat the unwanted communications.

I want to thank our panel of witnesses for joining us. I look forward to a robust discussion to understand the current landscape of illegal robocalls and robotexts plaguing U.S. consumers and businesses, so we can work together to identify and address remaining challenges.

[The prepared statement of Mr. Palmer follows:]

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

*Mr. Palmer. I now recognize the ranking member of the subcommittee, Ms. Clarke, for her opening statement.

*Ms. Clarke. Thank you, Mr. Chairman, and I thank our panel of witnesses for appearing before us today.

Americans are tired of hundreds of unwanted calls and texts they receive every year from scammers attempting to steal their hard-earned money. In 2023, Americans lost over $25 billion to phone-based scams. These criminals target the vulnerable and kindhearted by pretending to be law enforcement, Medicare, or even relatives in order to scam them out of hard-earned money. Enough is enough.

For years, there has been a bipartisan effort to address this issue. In 2019, Democrats and Republicans came together to pass the Pallone-Thune TRACED Act, giving the federal government greater enforcement ability and the authority to implement a call authentication framework and force phone carriers to improve the traceback of illegal calls.

Under the Biden Administration, the Federal Communications Commission created the Robocall Response Team that has assisted in cutting off providers who facilitate illegal robocalls. And last year, Ranking Member Pallone led a Democratic package to close the loophole scammers rely on to target Americans. Committee Democrats are now working on updates to strengthen that package.

Unfortunately, the Trump Administration and congressional Republicans are retreating from the fight against illegal robocalls and robotexts. Just last week, President Trump released his 2026 budget proposal, in which he recommends cutting $42 million and firing 83 people from the Federal Trade Commission. By the Trump Administration's own definition, the mission of the FTC is to protect the public from unfair or deceptive business practices, including unlawful telemarketing and robocalls. How can we expect the federal government to do more to protect Americans when the Trump Administration is firing the very people whose job it is to enforce the law?

Right now, law enforcement in all 50 states and the District of Columbia are combating robocalls. A bipartisan group of 40 state attorney generals (sic) wrote to Congress to say that their state laws regulating artificial intelligence help prevent spam phone calls and texts. But just a few weeks ago, Republicans on this committee voted for a reconciliation package that includes a 10-year moratorium on enforcement of state and local AI laws that these state attorney generals are opposed to. This provision stops states in their tracks from doing important work when we have not yet provided a federal solution.

I think my Republican colleagues forget they are not the only elected officials in this country. State legislators and law enforcement work in tandem every day to stop these harassing robocalls and texts, and you should not stand in their way.

Stopping robocalls and texts will require dedicated employees at every level of government. Congressional Republicans should not hamstring the efforts of state and local enforcement, and President Trump should not slash and burn the budgets and staff of federal agencies, all of which are dedicated to serving the American people. We in Congress have a duty to our constituents. Committee Democrats are here to prioritize the will of the people who put us in these chairs, not prove our loyalty to Donald Trump.

If my Republican colleagues honestly want to stop illegal robocalls and robotexts, let's work together to support the federal employees and agencies that work, instead of tearing them down.

Having said that, I thank you, and I yield back, Mr. Chairman.

[The prepared statement of Ms. Clarke follows:]

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

*Mr. Palmer. The chair now recognizes the chairman of the full committee, Mr. Guthrie, for five minutes for an opening statement.

*The Chair. Thank you, Chairman Palmer, and I thank the Ranking Member Clarke. I thank you for holding this hearing. A lot of times, when we are back from our breaks away from home, people in D.C. ask us, what are you hearing back home? And I will tell you, I mean, of all the things going on in Washington, D.C., one of the number one things I hear is robocalls.

And I was sitting with a good friend of mine who is a little older, and just chatting with him for about an hour during the break. And I bet his phone rang four or five times. And each one was a robocall. So this is important. It is important to the American people. And it is not just because of the annoyance, it is because of the people that get ripped off with these people. And there are over 52 billion robocalls, and that is 4 billion calls a month, an average of 13 calls per person.

At the outset, I would like to state that many robocalls are both legal and necessary. Robocalls are used to convey public service announcements and emergency messages. They are used for announcing school closures and providing reminders of upcoming appointments and payments. These are the calls that we want.

But a large number of robocalls are illegal and are used to defraud, harass, and deceive customers. We have all received calls where someone on the other end of the line pretends to be IRS or Treasury and attempts to offer student loans or debt relief and sell insurance, or claims to be a bank or a credit card company. According to one survey, American victims of fraud lost an average of $450 to phone scams that prey on trust and exploit vulnerabilities. This exploitation is despicable, and the impact on victims is tragic, and many have lost their entire life savings. And we know this must stop.

And thankfully, in 2019, the committee passed the bipartisan bicameral legislation which President Trump signed into law, the Pallone-Thune TRACED Act, to combat the epidemic of illegal robocalls. And I was proud to vote for that. The TRACED Act is an important law that provides the FCC and its partners with greater enforcement authority to hold illegal robocallers and bad actors accountable.

Since the enactment of the TRACED Act, the FCC has used this authority to issue additional rules, as well as civil and criminal penalties under the Telephone Consumer Protection Act. As a result, we have seen a downward trend in the prevalence of illegal robocalls.

In addition, the FCC continues to mandate the voice service providers implement STIR/SHAKEN, caller ID authentication technology, and provide robocall mitigation plans to the robocall mitigation database. Furthermore, in 2020, USTelecom's Industry Traceback Group, or ITG, was recognized as the single private consortium to trace back the origins of suspected illegal robocalls, helping us to stop these calls at their source. All together, we have seen some great work done by our federal agencies and their industry partners.

However, despite these strides forward, illegal and scam robocalls persist. We are even seeing a significant increase in unwanted scam and robotexts, which include messages alerting consumers to act on undeliverable packages and unpaid tolls, to name a few examples.

Complicating these issues are new developments in artificial intelligence, including voice cloning and deepfake technologies to impersonate individuals and generate scam phone calls and texts. Just last month, the FBI issued a warning about a malicious messaging campaign targeting government officials and their acquaintances by sending AI-generated voice messages impersonating senior U.S. officials to gain access to their data.

As challenges evolve, so too must solutions. The Committee on Energy and Commerce has been at the forefront of leading discussions, understanding challenges, and developing solutions to address issues with new technologies, and we will continue to do so throughout this Congress. Notwithstanding the complex landscape illegal scam robocalls and robotexts pose for customers, legitimate businesses, federal agencies and their partners, I am optimistic that Republicans and Democrats will continue to work together to develop common sense, bipartisan solutions to protect the American people from these fraudsters.

And I want to thank the witnesses for being here today. Thank you for taking your time to be here. And I look forward to your testimonies. And I will yield back.

[The prepared statement of Mr. Guthrie follows:]

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

*Mr. Palmer. I thank the gentleman

The chair now recognizes the ranking member of the full committee, Mr. Pallone, for five minutes for an opening statement.

*Mr. Pallone. Thank you, Mr. Chairman.

Combating the surge of unwanted robocalls and robotexts has been a priority of mine for years. And, as I appreciate Chairman Guthrie saying, in 2009, I led passage of the TRACED Act. And this law has helped protect Americans from predatory and annoying robocalls, and gave federal agencies better tools to fight back against fraudsters.

Despite these steps, Americans are still continuously bombarded by unwanted calls and texts that are not only annoying but cause real harm through fraud and scams. Technological advancements have supercharged fraud and made it easier and less expensive for scammers to make massive numbers of robocalls, to spoof caller ID information in order to hide a caller's true identity. They also use artificial intelligence to trick consumers to thinking they are talking to a relative in financial trouble, or to a trusted business offering assistance.

Now, Americans received over 52 billion robocalls in 2024, which is nearly 200 calls for every American adult. Scams targeting seniors are especially rampant and take many forms, including calls or texts claiming to be from grandchildren or law enforcement or Medicare, all aimed at bilking money from the senior citizen. And robotexts are increasingly problematic, using automated text messages that trick recipients into clicking damaging links, providing personal or financial information, or paying for fraudulent items or services.

And Congress has to continue to update the authorities we have given both to the FTC and the Federal Communications Commission to crack down on robocalls. We must also consider legislation focused on robotexts and provide our consumer protection agencies with adequate funding and staffing to hold bad actors accountable.

The TRACED Act gave the FCC increased authority to require carriers to implement a call authentication framework, and stepped up enforcement action against bad actors and directed carriers to develop better tools to protect their customers. But as technology evolves, fraudsters are finding new ways to scam Americans and abuse loopholes.

So last Congress, I led a Democratic effort that would expand anti-robocall protections and provide explicit protections against robotexts. And our bill also would have closed loopholes exploited by scammers, combated the use of AI for scams, and alleviated the robocall blocking technology for consumers. My colleagues and I are working on updates to strengthen that package and I am sure today's testimony will help inform our thinking on how to better protect consumers from unwanted robocalls and robotexts.

Now, I am sure there is uniform agreement on this committee that it is important to put an end to harassing and illegal robocalls and robotexts. But I have to say that actions by the Trump Administration do threaten our efforts to do just that. There is a regular effort to undermine -- essentially what is happening is the Trump Administration and, of course, the House Republicans, you know, are cutting funding and staff from the very entities that protect consumers. And, you know, this is all to give the big tax breaks to billionaires who do not need them.

And the problem is that while law enforcement and state governments have been active in combating robocalls and on working with industry to find technical solutions to address robocalls, last month the House Republicans supported the reconciliation bill that included a 10-year moratorium on state and local enforcement of their own AI laws.

So if this big tech effort becomes law, it could stop state attempts to develop innovative solutions to prevent illegal robocalls and texts. And I think it compromises America's financial wellbeing and hamstrings states who are working to keep their citizens safe.

Federal consumer protection agencies are vital components of this fight against the robocalls and robotexts. But since taking office, President Trump has attempted to remove Senate-confirmed FTC commissioners, reduce FTC and FCC staff, and that cripples these two important agencies' efforts to protect consumers. And Democrats have advocated for stronger authority and resources for both the FTC and the FCC, and for sensible guard rails to ensure consumer safety is at the forefront of strong enforcement by federal, state, and private partners. But House Republican budgets that have all these cuts, they are basically under-resourcing these agencies and the staff that would actually use the tools we have given them to fight against robocalls.

So, you know, I have to say, you know, obviously, this is not the way to protect consumers. And, you know, I always worry, and I am almost out of time, Mr. Chairman, but I just worry that, you know, whether it is the SUPPORT Act that is on the floor this week, or it is your efforts to talk about the need to address robocalls and texts, if you do not have the resources, if you do not have the staff, and the money is cut for these agencies, then it is not going to be effective, no matter what we do as an authorizing committee. And I am going to continually point that out because I think it is important.

I yield back, Mr. Chairman.

[The prepared statement of Mr. Pallone follows:]

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

*Mr. Palmer. I thank the gentleman.

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

[The information follows:]

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

*Mr. Palmer. We want to thank our witnesses for being here today and taking time to testify before the subcommittee. You will have the opportunity to give an opening statement followed by a round of questions from the members.

Our witnesses today are Joshua Bercu, Executive Director for Industry Traceback Group and Senior Vice President of USTelecom; Ms. Sarah Leggin, Vice President of Regulatory Affairs for CTIA; Mr. Stephen Waguespack, President of the Institute for Legal Reform and Senior Vice President of the U.S. Chamber Federation, State and Local Advocacy, at the U.S. Chamber of Commerce; and, finally, Mr. Ben Winters, Director of AI and Data Privacy for the Consumer Federation of America.

We appreciate you being here today and I look forward to hearing from you.

You are aware that the committee is holding and oversight hearing and, when doing so, has the practice of taking testimony under oath. Do any of you have any objection to testifying under oath?

Seeing no objection, we will proceed.

The chair advises you that you are entitled to be advised by counsel pursuant to House rules. Do you desire to be advised by counsel during your testimony today?

Seeing none, please rise and raise your right hand.

[Witnesses sworn.]

*Mr. Palmer. Seeing the witnesses answered in the affirmative, you are now sworn in and under oath, subject to the penalties set forth in Title 18, Section 1001 of the United States Code.

You may be seated.

With that, we will now recognize Mr. Bercu for five minutes to give an opening statement.

TESTIMONY OF JOSHUA M. BERCU, EXECUTIVE DIRECTOR, INDUSTRY TRACEBACK GROUP, AND SENIOR VICE PRESIDENT, USTELECOM; SARAH LEGGIN, VICE PRESIDENT, REGULATORY AFFAIRS, CTIA; STEPHEN WAGUESPACK, PRESIDENT, INSTITUTE FOR LEGAL REFORM AND SENIOR VICE PRESIDENT, U.S. CHAMBER FEDERATION, STATE AND LOCAL ADVOCACY, U.S. CHAMBER OF COMMERCE; AND BEN WINTERS, DIRECTOR OF AI AND DATA PRIVACY, CONSUMER FEDERATION OF AMERICA

TESTIMONY OF JOSHUA M. BERCU

*Mr. Bercu. Chairman Palmer and members of the subcommittee, thank you for the opportunity to testify today. Congress's leadership in passing the TRACED Act and maintaining strong oversight remains critical to ensuring the industry and government act with urgency to address this top consumer concern. Your commitment remains vital to sustain the vigilance, innovation, and coordination needed in our continued and evolving fight against scam calls.

I am Josh Bercu, Executive Director of the Industry Traceback Group, or ITG, which is the FCC-designated traceback consortium under the TRACED Act, and Senior Vice President at USTelecom.

Let me start with the bottom line. The TRACED Act worked. When Congress passed the TRACED Act, robocall complaints were nearing a crisis point, doubling at the FTC from 1.7 million in 2014 to nearly 4 million in 2019. Today, they are down more than 70 percent. FCC complaints are down 77 percent. That's real progress. It did not solve everything, but we now have tools and a mandate to fight back.

Over the past six years, we have built a framework that makes it harder and riskier for bad actors and criminals to infiltrate our networks. But it is neither hard nor risky enough and the threat is evolving. Fraud losses are rising, not because of mass robocalls, but because of targeted, more sophisticated scams. We have gone from fishing with dynamite to precision strikes. And that demands a more agile defense.

That is where traceback has come in. Since its inception, the ITG has conducted over 20,000 tracebacks. We help identify who's behind illegal calls, whether it is a robocall campaign, a spoof threat to a high school, or a scam impersonating a bank. Our work supports law enforcement and drives action.

When a rural high school in West Virginia received a threatening call, we worked with providers to trace the call path within hours, helping police confirm the call was not actually made locally, and safely reunite families.

The tools Congress empowered are as essential now as ever. Call blocking and labeling stops millions of illegal calls every day. Call authentication has made it far harder for bad actors to spoof numbers at scale. And pursuant to the TRACED Act, FCC rules now require all providers to know where their traffic comes from and take action when it is identified as unlawful, including through our tracebacks. The threat is evolving, so we need to keep evolving with the threat.

The good news? We're not starting from scratch. Here are three things we think Congress can do to help. One, build a unified national scam strategy. We need a national strategy and a central federal coordinator or task force to unify efforts, eliminate silos, and give industry a clear point of contact. That strategy should include international cooperation, including on traceback. We also need to treat call-based scams for what they are, crime. And it's crime that can only be fully stopped through cross-border criminal enforcement.

Two, strengthen the tools that work. Let's reinforce the existing framework, extend the FCC's traceback designation cycle and provide narrow immunity so we can plan, invest, and act decisively without being distracted or deterred by an annual administrative process or the risk of nuisance lawsuits. We've also worked on new tools to explore other aspects of unlawful calling campaigns and, with congressional backing, they could become permanent and powerful parts of the tool set.

Three, unleash and promote cross-sector collaboration. Some of the most meaningful progress we've made has come from collaboration. We've launched a pilot with banks and carriers to trace spoofed numbers pretending to be the banks, a model of the cross-sector collaboration we need more of.

But barriers can get in the way. Right now, providers may hesitate to share intelligence simply because rules and risks are not clear. A narrowly scoped safe harbor could change that, clarifying that sharing information to prevent fraud is not only allowed but encouraged. Blame will not stop fraud, but partnerships can. The TRACED Act was a turning point, but we need to keep adapting and fighting back.

Thank you for your leadership. I look forward to your questions.

[The testimony of Mr. Bercu follows:]

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

*Mr. Palmer. The chair now recognizes Ms. Leggin for five minutes for your testimony.

TESTIMONY OF SARAH LEGGIN

*Ms. Leggin. Chairman Palmer and Guthrie, Ranking Members Clarke and Pallone, and members of the subcommittee, on behalf of CTIA and the wireless industry, thank you for the opportunity to testify today.

CTIA commends the committee for its leadership in protecting Americans from the scourge of illegal and unwanted robocalls and robotexts. Consumers rely on wireless more than ever for voice calls and text messaging. As reported last year, Americans devoted nearly 2.4 trillion minutes to voice calls, and they exchanged more than 2.1 trillion text messages. And texts have a 98 percent open rate, evidencing just how much consumers open and read and trust their texts.

Unfortunately, bad actors know how much consumers value and rely on wireless voice and text messages. As they have increased their deceptive efforts, we have increased our efforts and our success in combating them. So today, first, I want to talk about how we are working to stop robocalls, and then I will turn to the similar but different challenges we face when it comes to robotexts.

First, on robocalls, we appreciate the committee's actions through the TRACED Act to provide the FCC with new tools to combat illegal robocalls. Under this framework, the wireless industry is helping lead the way in advancing consumers' control over the voice calls they receive. Although automated calls from your pharmacy, school, or charity can be helpful and enhance consumer welfare, too many of them are intrusive and a consumer pain point.

In response, the wireless industry has built a range of defenses against illegal and unwanted robocalls. We spearheaded the development of STIR/SHAKEN authentication framework, led the way in implementing it, as the TRACED Act directed. In addition, wireless providers and their partners have launched a variety of powerful tools to regain consumer control over the calls they receive. These include know your customer practices, innovative call blocking, tracing back illegal robocalls to identify bad actors, and robust robocall mitigation programs.

Wireless providers black label or identify over 45 billion scam calls every year while also working hard to make sure that legitimate calls are completed. Thanks to these efforts, robocall complaints reached a six-year low last year. And we look forward to continuing progress there.

Now, turning to text messaging. Wireless text messaging is one of the most popular and trusted forms of communication among American consumers today. The wireless industry and our partners in the messaging ecosystem work really hard to keep it that way. To do so, we use proactive, multilayered measures that include tools like up front vetting and verification, sophisticated machine learning and AI for filtering and blocking, and consumer reporting, all balancing the need to protect consumers and ensure that legitimate texts go through.

As just one metric, wireless providers blocked over 55 billion texts last year, while at the same time delivering trillions of legitimate texts. And we are always evolving our techniques to leverage the latest technology and meet new challenges. We complement these tools with best practices that offer industry-led guidance to honor consumer preferences focused on consent while supporting legitimate communications. The best practices are adopted throughout the messaging ecosystem and were recognized by a coalition of consumer advocate organizations as a critical element in protecting consumers and the messaging platform from bad actors.

Notwithstanding all these efforts, bad actors continue to try to exploit consumers' trust by spamming and scamming them. So to better target those bad actors, CTIA launched the Secure Messaging Initiative, or the SMI, to convene the texting ecosystem to help identify scam activity and refer it to law enforcement for investigation. Through the SMI, we've already traced over 172,000 robotexts and made over a dozen referrals to our law enforcement partners at the FCC, FTC, DOJ and 50-state attorney general enforcement task force.

These focused on scams like student loans, government and bank impersonation, package delivery, and more. Collectively, these efforts are helping to stop scammers and maintain consumer trust in text messaging.

Collaboration with our government partners is key to continued success and we support the administration's efforts to protect consumers. Chairman Carr at the FCC has made cracking down on illegal robocalls a top priority and we support this effort. And we acknowledge Ranking Member Pallone's Do Not Disturb Bill with the goal of combating consumer fraud.

Finally, we encourage Congress to take steps to support action against the bad actors behind illegal robocalls and robotexts. Many agencies are working hard to fight consumer fraud but lack the personnel or resources to bring cases. To help out, Congress could have agencies report on their current consumer fraud resources and actions and leverage that information to prioritize support. With more resources at the federal and state levels, Congress can help take bad actors off the field and stop illegal robocalls and robotexts at the source.

Thank you for the opportunity to testify today. We look forward to working with you all to protect consumers from intrusive and illegal robocalls and robotexts.

[The testimony of Ms. Leggin follows:]

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

*Mr. Palmer. The chair now recognizes Mr. Waguespack for five minutes for your testimony.

TESTIMONY OF STEPHEN WAGUESPACK

*Mr. Waguespack. Thank you, Chairman Palmer, Ranking Member Clarke, and members of the subcommittee. My name is Stephen Waguespack and I serve as president of the U.S. Chamber of Commerce's Institute for Legal Reform, more commonly known as ILR. The ILR is a division of the Chamber whose mission is to champion a fair legal system that promotes economic growth and opportunity. We believe that an effective legal system is critical to helping both customers and business owners. Thank you for the opportunity to testify today about the robocalling landscape and how American businesses are protecting consumers.

There are four main points I would like to cover in today's hearing. Number one, legitimate businesses support and are helping to lead efforts to crack down on illegal and abusive robocalls and robotexts. Businesses have every incentive to ensure that consumers continue to trust these communications. The illegal calls and texts that seek to defraud U.S. consumers begin with bad actors exploiting the reputation and good will of trusted American brands.

For example, one in three businesses report being impersonated by scammers, with 13 percent reporting a switch in brands due to this deception. According to 2024 data from Hiya, 45 percent of consumers have received a call from someone impersonating a legitimate business, and 70 percent of businesses report getting a similar attack. Beyond reputational damage, fraudulent calling and texting schemes also degrade consumers' trust in these types of communications, making it difficult for businesses to engage with their customers. That's why many companies are proactively helping regulators trace these bad actors and going on the offensive by fighting back directly against them.

For example, Marriott International brought its own trademark lawsuit against malicious robocallers and scored significant legal victories over both foreign and U.S.-based defendants, while DirecTV also secured a total of $8 million in judgments and broad, permanent injunctions. The private sector is also devising innovative technologies, such as analytics-powered software, while partnering with the government through programs like the Industry Traceback Group and Secure Messaging Initiative in tackling illegal and abusive robocalls.

Number two, more legislation will not solve the problem. Fraudulent and abusive robocalls and robotexts are already illegal. Congress must ensure that its already substantial efforts to curb these activities bear fruit by encouraging federal agencies to make illegal robocalls and robotexts an enforcement priority. As the Chamber has previously urged, lawmakers should push DOJ to prioritize enforcement against these bad actors and report annually to Congress on their efforts.

There is optimism that focus on this topic could be welcomed by the DOJ, as we have seen the FCC and FTC utilizing tools like the traceback program to increase the focus on bad actors.

Number three and most critically, the TCPA's private rights of action provisions continue to fuel abusive litigation against American businesses. This difficult operating environment hurts both businesses and consumers and is undermining the proactive efforts by this Congress to address the very real problem of scammers. The private right of action provisions in the TCPA make it more challenging for legitimate businesses and organizations to send and for consumers to receive good calls and texts, such as appointment reminders, notifications about school closures, and other communications that consumers want. At the same time, it does not deter bad calls and texts, such as fraudulent and harassing communications that originate from bad actors.

It is critical that Congress distinguish between these two types of calls and limit the ability of a handful of aggressive plaintiff firms to dominate the market for these suits. Congress should also encourage the FCC to simplify

TCPA regulations to boost compliance, ensure certainty for legitimate businesses, and focus on addressing bad actors.

Fourth and finally, Congress could utilize the precedents set in other federal and state statutes to limit the abuse of private rights of action found within TCPA by implementing, one, reasonable damage caps; two, clear safe harbor provisions; three, limits on unreasonable attorney fees; and, four, mandatory disclosure of any usage of third party litigation financing known as TPLF in these TCPA cases to ensure consumer rights are protected. The business community wants to end illegal robocalls and robotexts to foster a safe and trustworthy communications ecosystem for businesses and their consumers.

As Congress considers pass forward, the enforcement should be a top priority of all federal agencies, and Congress should consider reforms to prevent legitimate businesses from being ensnared in abusive TCPA litigation. Thank you for your work to date on this topic, and to the subcommittee for the opportunity to discuss these important issues. I look forward to answering your questions. Thank you.

[The testimony of Mr. Waguespack follows:]

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

*Mr. Palmer. The chair now recognizes Mr. Winters for five minutes for your testimony.

TESTIMONY OF BEN WINTERS

*Mr. Winters. Chair Guthrie, Ranking Member Pallone, Chair Palmer, Ranking Member Clarke, and members of the subcommittee, thank you for inviting me to testify before you on this important issue.

I am Ben Winters. I am the director of AI and privacy at the Consumer Federation of America, or CFA. CFA is an association of nonprofit consumer organizations established in 1968 to advance the consumer interest through research, advocacy, and education.

There is a staggering amount of monetary and emotional harm caused by scams perpetrated through robocalls and robotexts. Consumers lost over $12.5 billion to scams last year, which was a 20 percent increase from 2023. Even when no money is lost, there is a constant sense of annoyance and need for vigilance. Americans received an estimated 19.2 billion robotexts and 5 billion robocalls last month alone. And just this morning, the Washington Post featured the fact that there is a five times jump in scam losses from schemes that started in texts since 2020.

In this testimony, I will be highlighting how underregulated technologies like AI are making these problems worse, how federal consumer protection agencies can be doing more, and how Congress can act to protect consumers from this annoying and dangerous problem.

Generative AI reduces the time and effort criminals have to expend in order to deceive their targets. Products like ChatGPT can create quick and unique human-sounding scripts that can be sent in text or read by humans or AI-generated voices, and it's easy to make variations that make them difficult to spot.

In CFA's recent "Scamplified'' report, we illustrate how easy it is to use ChatGPT to generate text with an urgent ask to add $50 worth of bitcoin to a wallet. It spat out 30, 50, 100 texts with common women's names and real hospitals in common U.S. cities to create urgency. It even continued to spit out texts when we asked it to target it to someone that might have dementia.

And it is not just text generators. Voice cloning tools can now replicate anyone's speech using just a few seconds from a phone call or a podcast interview. Scammers have exploited this to impersonate loved ones such as in grandparent scams you have already heard about today.

Consumer Reports' investigation showed popular voice cloning platforms do not require the user to verify their identity or gain consent before creating these voice clonings.

Beyond AI, there is a host of companies in what we call the scam stack, all of which are fueling an increase in scams. These include data brokers that sell data en masse based on people's behavior, purchases, relationships, location, and more, automated content delivery, things like we're talking about today, and methods of reporting which can be improved to bridge the gap between a victim and the authorities that could help.

Federal consumer protection agencies tasked with stopping scam robotexts and robocalls like the FCC and FTC are being stripped down and distracted. The consequence is stark. In April, the Department of Justice eliminated their consumer protection branch entirely. This is the branch that brought a landmark criminal case against a data broker that sold over 30 million records of elderly Americans that was then used to perpetrate a scam. This type of enforcement of upstream actors is exactly what we need to see, and it is troubling to see that agency get axed.

Americans deserve an FCC that is focused on the complicated robocall ecosystem, and they have done a lot to try to address it. But the agency leadership right now seems focused on controlling the speech and hiring practices of entertainment companies that are perceived to be the enemies of the President, instead of ramping up rulemaking an enforcement as an independent agency.

Chairman Carr's Delete, Delete, Delete Initiative, in which he is asking the American public what regulations the

FCC should delete because they stand in the way of expansion and technological innovation is illustrative of this disastrous deregulatory approach that does not even mention consumer protection.

At the FTC, the firing of key staff and critically two of the five commissioners have left the agency ill equipped to protect American consumers. The agency must finalize the individual impersonation rule so they can deter and enforce violations of widespread things like voice cloning, like they have started to do with government and business impersonation, which they finalized last year.

Both agencies must prioritize enforcement against upstream actors, such as voice service providers and AI developers who knowingly facilitate these harmful practices. These intermediaries are critical to how illegal calls and texts scale and are essential to meaningful accountability.

Congress has to hold upstream actors accountable, just like I talked about, strengthen enforcement tools beyond just what's in the TRACED Act, increase transparency, and mandate consequences for known bad actors throughout the call path. We also urge Congress to increase funding for state enforcement, pass privacy laws restricting data brokers, and require responsible AI moderation and transparency.

One thing Congress absolutely should not do right now is pass a moratorium on regulating AI at the state level. The scale of these problems is one of many reasons it's not the time to do this. And if states can create transparency or establish appropriate liability, we should welcome it, embracing the critical roles of states not only to protect consumers but be the laboratory of democracy.

Right now, the FTC, FCC, and CFPB risk being cops off of their beat. And Congress must empower them, resource them, and restore them in order to aggressively protect consumers. The American people deserve nothing less.

Thanks again for the opportunity to testify, and I am happy to answer any questions you might have.

[The testimony of Mr. Winters follows:]

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

*Mr. Palmer. I thank you all for your testimony. We will now move on to questioning. I will begin and recognize myself for five minutes.

Mr. Bercu, the Broadband Association's Industry Traceback Group conducted more than 3,600 tracebacks of suspected unlawful robocalls in 2024. Generally speaking, what percentage of unlawful robocalls are foreign originated?

*Mr. Bercu. Thank you for the question. So I do not have an exact number on how many came from foreign countries or foreign entities. But we do know that a lot of the fraud comes from abroad. Illegal telemarketing, we see that sometimes originate at home, sometimes abroad. But a lot of the fraud does originate overseas.

And one of the things we have been seeing a lot lately is, because so much of enforcement and regulation was focused on who brought the illegal call into the country, what we're now seeing is some of the bad actors spinning out U.S.-based LLCs so that we are tracing it to a U.S. entity that probably has no people in the United States at all.

*Mr. Palmer. Dealing with the foreign actors, though, creates some tremendous challenges because we cannot charge them with a crime right now, unless they are operating in country. Is there any recourse through civil action? I mean, what recourse do you have to deal with foreign actors? And be as brief as you can.

*Mr. Bercu. Yeah, I think we can do criminal action, and I think that needs to be a priority. The same people attacking us here are attacking other countries as well. I think there's a lot of opportunities for collaboration. And just to give you one anecdote, when the FBI did work several years ago with the Central Bureau of Intelligence in India to raid some of the call centers there, we saw IRS robocalls drop 80 percent overnight.

*Mr. Palmer. Ms. Leggin, can you tell us how CTIA's secure messaging initiative works to trace back robotexts? And how effective has this been to stop illegal and unwanted robotexts?

*Ms. Leggin. Thank you for the question. CTIA's secure messaging initiative was launched to convene the messaging ecosystem and the various players that have a role there in protecting consumers so that we can facilitate information sharing among the industry stakeholders to complement their existing industry tools to better fight the bad actors, and then to share that information with law enforcement partners at the FCC, FTC, DOJ, and the 50-state attorney general enforcement task force. To date, we have done over 172,000 robotexts as part of those information packages that we share with law enforcement. And we've done over a dozen of those packages that focus on scams that you all have seen, including government or bank impersonation, package delivery, and AI-enhanced scams as well.

We continue to focus on the areas where we're hearing that scams are happening for consumers so that we give that information to law enforcement so they can prioritize their efforts to go after the bad actors and stop the traffic at the source.

*Mr. Palmer. Mr. Bercu, I want to go back to you. How widely has the STIR/SHAKEN caller ID authentication framework been implemented? And what percentage of the providers still need to implement the framework?

*Mr. Bercu. So under FCC rules, it is implemented on the IP portions of providers' networks. And we have seen a shift in practice because of it, especially the high-volume illegal telemarketers. One of the things, I think, because of STIR/SHAKEN, they've moved away from spoofing to actually getting real numbers, which STIR/SHAKEN does not directly address.

*Mr. Palmer. Mr. Waguespack, in your testimony, you were talking about how the private right of action has been abused. Instead of protecting people who have been harmed by scam robocalls, it has led to basically a cottage industry that is attacking legitimate companies. Can you talk a little bit about that?

*Mr. Waguespack. Thank you, Mr. Chairman. Well, in the statements from the opening statements from the panel and obviously from the witnesses here, there seems to be a unified focus that these bad actors a lot of times which are very hard to find which are located overseas, those are the true ones driving a lot of this issue. The private right of action provisions within TCPA are not utilized to go after those bad actors. Instead, a cottage industry has developed to go after simply where there are opportunities to make money.

And also the provisions of the PRA within TCPA are extremely broad compared to other federal statutes. There is no caps on recovery, as you see in HIPAA, no safe harbor provision you see in COPPA, no cap on attorney fees that you see in other statutes. And so it has created a class action factory that is being exploited by just a handful of firms --

*Mr. Palmer. So it has become a predatory use of the private right of action. I saw where one of the judgments was for $260-something million. So how do we respond to that?

*Mr. Waguespack. I think we borrow from other statutes already in place at the federal level. You look to HIPAA to put a cap on the total recovery. They set that at 25,000. There is no cap here. It is up to 15,000 per occurrence under this statute, which absolutely drives those numbers up.

And most of these suits, they are not trying to win in court; they are just trying to drive discovery to make it very expensive and drive settlement. And you are seeing it play out time and time again. In fact, there is one law firm that has done over 155 cases over a three-year period on this front. They have developed a niche market. There is even one plaintiff who has done almost 125 himself on this issue.

So you have a handful of folks exploiting this system. That is not helping the consumers that desperately need some of the help from these scam robocalls.

*Mr. Palmer. Thank you.

The chair now recognizes the ranking member of the subcommittee, Ms. Clarke, for five minutes for her questions.

*Ms. Clarke. Thank you, Mr. Chairman.

Unwanted calls continue to be the top consumer complaint received by the FCC, the Federal Communications Commission. In 2024, Americans received over 52 billion robocalls and 49 percent of those robocalls were scams or from telemarketers.

Mr. Bercu, how has the robocall and robotext threat landscape changed since the implementation of the TRACED Act and STIR and SHAKEN?

*Mr. Bercu. So I think we have made a lot of progress. But as you are recognizing, there is work left to do. We have seen complaints. They are still too high, but they have dropped pretty dramatically from the highs from several years ago.

We have seen some of the bad actors, instead of for scam robocalls, they are about 50 percent of what they once were for scam robocalls. But we have seen the scammers move from mass robocalls to more targeted, more sophisticated attacks where they know exactly who they are calling. So that is a little bit of how this has changed over time.

*Ms. Clarke. Thank you. So we still have more to do.

With the work left undone in the fight against phone scams, it baffles me that the Trump Administration is undermining the government institutions that combat them. In March, President Trump attempted to illegally removed Senate-confirmed commissioners from the Federal Trade Commission, an independent agency with the explicit mission to protect the public from unfair and deceptive business practices like unlawful telemarketing and robocalls. And in April, in accordance with a Trump Administration instruction, the Department of Justice announced plans to dissolve its consumer protection branch, which tries cases targeting large-scale scams against seniors, AI, and cybercrimes against consumers, and illegal telemarketing. This just makes no sense.

The Consumer Financial Protection Bureau, FCC, FTC, and the Department of Justice have all been hit by early retirements, terminations, and deferred resignations. And they are all agencies that combat the robocall problem we are gathered to discuss today.

Mr. Winters, how does an unstable and depleted FCC and FTC workforce impact the role both agencies play in addressing the robocall scams?

*Mr. Winters. Thanks for the question. I mean, these under-resourced consumer protection agencies is just a big win for scammers, right? Less cops on the beat mean less consequences, and they can sort of act with impunity. And so what we need to be doing, and I think was reflected in all of our testimony today, is that we need more enforcement, more resources, and more proactive behavior. And everything from firing commissioners to budget cuts goes exactly against that.

*Ms. Clarke. Thank you. Last week, President Trump released a detailed Fiscal Year 2026 funding proposal. If enacted, this proposal would make permanent and add to the number of fired federal employees, including 74 at the FCC, 83 at the FTC, and 32 of which are identified as consumer protection roles. The proposal also cuts 42 million from the FTC and more than 18 million of which would go directly toward protecting consumers.

Mr. Winters, what would happen to the robocall fighting infrastructure if the federal government pulled back from its role, whether it be from a lack of manpower, funds, or general disinterest in holding scammers accountable?

*Mr. Winters. In the interest of time, I'll be simple, in that it will get worse.

*Ms. Clarke. And what do the government actions we have discussed today tell the scammers and fraudsters who conduct robocalls and texts about the priorities of the U.S. government? Do you think actions like these make robocalls more likely to occur in the future?

*Mr. Winters. Yeah. I mean, I think it incentivizes bad behavior. It makes people feel like we are absolutely not going to be able to -- we're not going to get enforcement action against us, it is going to be hard to track. It is hard to track when you have a full-court press against it, and we have seen that for years. But if we are pulling back, then that is even, you know, an unimaginable harm for American consumers.

*Ms. Clarke. Very well. Well, Mr. Chairman, in their written testimony, several of today's witnesses said Congress must increase support for and prioritize enforcement actions if we truly want to stop bad actors. The experts are calling for more funding and enforcement, not less. And I ask my colleagues across the aisle to listen to them.

With that, I yield back.

*Mr. Balderson. [Presiding] Thank you, Ms. Clarke.

Next is the Chairman of the Full Committee, Mr. Guthrie.

*The Chair. Thank you. I thank all the witnesses for being here. I appreciate you all being here this morning.

So, Mr. Bercu, in July of 2020, the FCC first selected USTelecom, the Broadband Association's Industry Traceback Group, as the single registered consortium to conduct private led traceback efforts, and has redesigned USTelecom's ITG each year since.

So could you kind of explain -- I know I am going between two hearings, so if you are repetitive, it helps me to repeat anyway, so how does traceback work and how has the USTelecom ITG helped the FCC with its efforts to fight illegal robocalls?

*Mr. Bercu. Yeah, absolutely. So traceback helps solve for one of the problems, which was when a call is spoofed and we do not know where it is coming from, the carrier does not know exactly where it came from -- STIR/SHAKEN helps with that, but traceback goes even farther. And we go hop by hop in a semi-automated system through a portal, and we find out exactly where it is coming from. And in fact, in our tracebacks, we have identified over 2,000 providers from 75 different countries. So we will trace it all over the world until we can find out who is making the calls and actually disrupt it there.

Our data has been used for virtually every robocall enforcement by the FCC, by the FTC, by the state AGs, so it has been a very successful partnership with the industry and government.

*The Chair. Well, should the technology not be in place to say if I am sitting in Bowling Green, Kentucky, and a phone call is coming in from Nigeria that is not in my data in my cell phone or anything like that, should that be -- there is technology that can block that from coming. I mean, you have to sign up for it, I gather, but there is technology that keeps that from coming to your phone, does it not?

*Mr. Bercu. So the challenge is that there is not perfect information at the carrier side about where that call is coming from. STIR/SHAKEN helps with that. I am optimistic that a recent rule clarification the FCC did last year, that will continue to advance STIR/SHAKEN and the impact there. But that is the challenge. And so there's definitely tools to achieve that, but the carriers do not have perfect information to know that call is coming from Nigeria.

*The Chair. My understanding is that when a lot of these robocalls happen, they are not like I am calling Neal Dunn in Florida and faking him out on something, like I am a criminal in Bowling Green calling Neal Dunn in Florida. It is usually, spam is just thousands of calls instantaneously going out. Can carriers not determine that and block those calls?

*Mr. Bercu. So that type, it still happens, but that is at a fraction of what it once was, thanks to enforcement, thanks to the TRACED Act, thanks to STIR/SHAKEN. Those types of calls are down, depending on the data you look about 50 percent.

Where we see fraud calls, a lot of the robocalls that people still hate, a lot of those are illegal telemarketing. That is the majority of the robocalls people get, where it is telemarketing that no one consented to and they are violating the TCPA.

But what we are seeing with the scams are the scams are getting more sophisticated, more targeted, where they are targeting individuals.

*The Chair. Okay, so Ms. Leggin, could you talk about how the CTA is trying to help fight these spam calls and robocalls?

*Ms. Leggin. Sure thing. Thank you for the question.

As Josh said, the --

*The Chair. I think you probably need your mic. There you go.

*Ms. Leggin. Try that again?

*The Chair. Perfect. It was on?

*Ms. Leggin. Is it on now?

*The Chair. Maybe just closer to it. Yeah, closer to it.

*Ms. Leggin. Sorry. Cannot see if it is on or not.

Thank you for the question.

Like Josh's members, the wireless industry are dedicated to protecting consumers from illegal and unwanted robocalls. We helped lead the way in developing the STIR/SHAKEN framework, and we supported this committee's efforts through the TRACED Act to promote the deployment of that. And it is now working well as a call authentication tool to help protect consumers from spoofed calls. It is just one tool in the toolbox, though, so especially over the last few years, we have been developing lots of different call blocking, labeling, filtering tools to complement STIR/SHAKEN as part of a multipronged approach to protect consumers from robocalls.

At CTIA, we are developing the next generation of call authentication, which is branded calling or RCTA's BCID, or branded calling ID, which gives consumers even more information about who is calling and why, to help empower consumers about whether to answer the phone again, as well as protecting them by providing consumer resources to educate them about which calls to ignore so that we are kind of coming at it from all fronts.

*The Chair. I assume that could be a competitive thing between providers to say, hey, if you use our service, we can help you block your robocalls. I assume that would be.

So Mr. Waguespack, how about increasing fines for illegal robocalls? What would that -- would such a change affect legitimate businesses? And how could we improve collection of existing fines or overall enforcement?

*Mr. Waguespack. You know, obviously, FCC and FTC, I think, have done a really great job working with industry partners to develop through traceback and other initiatives to identify those, so we definitely encourage strong enforcement. And add that DOJ should also go after these bad actors any way we can. We think going through those channels as compared to unleashing a small niche cadre of plaintiff firms to go after quite frankly credible businesses just because they cannot find the bad actors has been the wrong minor approach within TCPA.

So it is that private right of action that truly we think is a disincentive to businesses to reach out to develop those partnerships with their consumers that, quite frankly, most of their consumers want.

*The Chair. Okay, thank you. Well, my time has expired and I yield back. Appreciate you all being here. Thanks.

*Mr. Balderson. Thank you, Mr. Chairman.

Next up is the ranking member of the full committee, Mr. Pallone.

*Mr. Pallone. Thank you so much. And, look, I think we all know we have to do more to stop these dangerous and unwanted calls and texts that continue to bombard Americans. I mean, I get so many myself every day. And they are not just harassment, they are causing real harm. The phone scams alone defrauded Americans of $25 billion in 2023.

Now, the TRACED Act, which I authored in 2019, required the implementation of the STIR/SHAKEN call authentication technology to help verify the legitimacy of calls. So I wanted to ask Mr. Bercu, you run the Industry Traceback Group which traces calls to their origin as required by the TRACED Act on behalf of the communications industry. In your testimony, you discuss how industry is utilizing this framework to fight the problem of robocalls and to protect consumers from scam artists.

What more can industry do to protect consumers from unwanted and dangerous robocalls and robotexts? I am going to ask you a question and then Mr. Winters, so a couple minutes.

*Mr. Bercu. Sure. So thank you for the question, Ranking Member Pallone.

I think the industry, we do have blocking and labeling deployed. We do -- STIR/SHAKEN is deployed. I think there is a lot at work there. But I think what our experience shows is that when we are dealing with whether it is the illegal telemarketers, whether it is the criminal fraudsters abroad, they do not stop because it gets a little bit harder. This is their business so they keep trying to find new paths.

So I think what we see with Traceback, we are tracing them back. We have adapted to tracing back the targeted scam calls, working closely with the financial sector, other sectors as well. And I think that is more of the work to be done, complemented by very aggressive enforcement against the actual bad actors.

*Mr. Pallone. Thank you. So in March, President Trump illegally, in my opinion, fired the two Democratic FTC commissioners, meaning that their crucial voices are missing from any discussion at FTC of how to better protect consumers from robocalls and robotexts. And they have my full support in their ongoing lawsuit to be rightfully restored at the FTC, and I think that is the very first step that needs to be taken.

But just last year, I introduced, and I mentioned also the Do Not Disturb Act, a comprehensive piece of legislation that aims to build on the success of the TRACED Act. And it would ensure that scam artists using illegal robocalls or robotexts cannot exploit new loopholes as new technology makes it even easier for fraudsters to steal from Americans.

So, Mr. Winters, I have two questions. You have two minutes.

Do you agree there is a need for legislation to provide updates to current laws like last year's Do Not Disturb Act, and do the FTC and FCC need more authority from Congress to fight text message scams? Is it just money and enforcement, or do they actually need more authority, if you will?

*Mr. Winters. Thank you. Yeah, so on that first question, I think there is a lot more that Congress can do, and there is more that they need to do. And so whether that is some of the provisions in the Do Not Disturb Act, like codifying the rule about AI disclosures and increasing penalties for AI-generated scam calls, there is a lot more that can be done by Congress including giving more resources to not just FCC but to state attorneys general, who are leading the forefront of a lot of this work, and increasing collaboration.

*Mr. Pallone. But do they need more authority, though?

*Mr. Winters. They do need more authority. One thing in particular is that they are not able to directly collect fines. They have to refer fine collection to the Department of Justice. And so they have to rely on another overworked agency to collect fines. And we see a lot of times, although there are big headlines and numbers of fines, the FCC might not actually be able to resolve and get a lot of that money back. So that is one thing that needs to be done in terms of authority.

And they also need the authority to put more automatic suspension and provisions in the robocall mitigation database, so that when there are repeat bad actors, they are automatically taken out. They cannot just stay in the robocall mitigation database. There is not enough sort of continued standards and continued enforcement using that.

*Mr. Pallone. Well, thank you. And, Mr. Chairman, as you can see, I think there is a question more authority is needed for the agencies. But I will repeat what I said earlier, which is they also need more resources and staff and cutting back on staff and firing, you know, some of the commissioners is certainly not the way to go if you really want to try to improve the situation with robocalls. And so I would not only ask that we try to move toward more authority to fight these scams, but also provide the resources, not cut the resources, not cut the staff.

And with that, I will yield back.

*Mr. Balderson. Thank you, Mr. Pallone.

I am up next. So welcome everybody. I am glad you are able to join us.

Ms. Leggin, I will direct my questions to you this morning.

According to the FCC, text message scams have increased 500 fold in recent years. How have scams become more sophisticated over the years?

*Ms. Leggin. Thanks for the question. CTIA and our members are dedicated to protecting consumers from scam and spam text messages while also making sure that legitimate ones go through, because we know that consumers open and read and trust their text messages, as one of the most preferred platforms for communications today.

Over the years, we have seen bad actors increasingly target text messaging because they know that consumers open and read those texts. So as bad actors have evolved and enhanced their tactics, we've evolved and enhanced our defenses as well. So over the years, we've enhanced our blocking, filtering tools by enhancing them with machine learning and AI. We have launched the Secure Messaging Initiative, which is our work to partner with law enforcement to give them actionable information about bad actors so that they can go and take traffic off at the source, and those are working to help the FCC, the FTC, DOJ, and the attorney general enforcement task force in giving them information they can go after bad actors with.

*Mr. Balderson. Okay, thank you very much. You also answered my follow up.

Are mobile carriers and other industry players doing enough to address the growth in scam and illegal robotexts?

*Ms. Leggin. Our industry is really dedicated to this issue. As just one metric, we blocked over 55 billion texts last year, while also making sure that the legitimate ones go through, and supporting over 2 trillion legitimate texts. So it really is always a balance. But we've dedicated a lot of different resources to enhancing our protections against bad actors.

In terms of more things we can do, again, we can welcome help from Congress in prioritizing resources towards enforcement so that the agencies we work with can take on more of those cases, do more investigations, and go after the bad actors to stop that traffic at the source.

*Mr. Balderson. All right, thank you.

How well are mobile carriers engaging with states and other entities for information sharing and enforcement? For example, with the scam toll text, did mobile carriers pause delivery and contact state toll authorities to verify the legitimacy of the numbers?

*Ms. Leggin. Our members were focused on the toll road scams as well as the other versions of that as part of our work to protect consumers from all those types of scams that impersonate legitimate businesses.

The wireless carriers as well as other partners in the messaging ecosystem, including providers of other types of messaging apps that were targeted by that type of scam, including over-the-top online-based and at-base messaging all were working together to share information with law enforcement to help them find the bad actors responsible and take them off the field.

*Mr. Balderson. Okay, thank you. How can we get mobile carriers to better engage and pull their weight to stop the flood of robotexts at the same level as robocalls -- at the same level they dd for robocalls? I'm sorry.

*Ms. Leggin. The wireless industry and our messaging ecosystem partners are really focused on this issue. For years, we have been seeing bad actors really target the voice network because there were not blocking and other protections in place until the last few years.

In text messaging, we have actually had the ability to block and to filter and to employ up-front vetting and verification for decades. And so for a long time, the messaging platform was really protected from bad actors. Of course, bad actors are getting more sophisticated and over the last few years targeting text messaging more. But this has been an area of focus and a priority for our members for years. And we continue to dedicate significant resources toward protecting consumers while maintaining trust in text messaging.

*Mr. Balderson. Okay, thank you very much. I yield back my remaining time.

Next up is the gentlelady from Colorado, Ms. DeGette.

*Ms. DeGette. Thank you so much.

So I just got back along with many of our colleagues on this committee from a conference on artificial intelligence. And so I would like to talk with you about that today, because I think it is really being implemented in a disturbing way by scammers to find new ways to deal with Americans. A lot of us have been hearing these chilling stories about how somebody gets called by somebody who they think is their child or their parent and asked for money, and the voice sounds eerily like their loved one.

So, Mr. Winters, I want to ask you, how has AI technology been used to create more sophisticated robocall and robotext scams that target consumers?

*Mr. Winters. Thanks for the question. It has been in a lot of different ways, and so I will categorize the two different types of AI systems in it. So one in text generation services, like sort of as I mentioned in my opening statement, whether it is something like ChatGPT or cloud that you might have played around with, or one of the ones that even has less moderation, you can create a bunch of texts really quickly that have good grammar and, you know, seems like -- you do not have the bells going off in your head from them. So you can do that.

You can have a list of people's names, target based off their location, other information you have, have it connect to a link of, you know, a wallet or a Zelle or something like that. So it is just a sort of scale and accuracy and plausibility thing.

The other big category is the sort of impersonation of people, whether that be through voice or video. And that is where you see the really harrowing stories of sort of like realtime fraud and deepfake stuff that, you know, have not only caused a lot of emotional harm but have sort of ruined people's lives. Yeah.

*Ms. DeGette. So this kind of goes without saying. But because of this degree of sophistication, even when you have an educated consumer, it becomes much more difficult to identify these scams?

*Mr. Winters. Absolutely. I mean, I think that one thing is it is really difficult and kind of an impossible proposition to have all American people be able to spot when something is AI in the moment and then not respond to the emotional sort of "I'm your son and I'm in jail'' thing, even if you are able to flag that. And then not all AI-generated anything will be a scam or a fraud, so it is complicated there. Because you do not necessarily want to teach that, or it will just get people paranoid. So it is really -- it should be on the companies and on the enforcement --

*Ms. DeGette. Right, so if we are not going to rely on the consumers by education, Ms. Leggin, what more can industry do to filter these messages and prevent them from ever getting to the victims?

*Ms. Leggin. So as Mr. Winters said, it is a balanced approach to make sure that we are blocking the messages that we do not want consumers to receive and they do not want to receive, while also making sure that legitimate ones go through.

*Ms. DeGette. That is right.

*Ms. Leggin. So with AI-enhanced scams, for example, there are aspects of that that we can also detect using AI by analyzing vaster quantities of data, by enhancing our existing tools and algorithms and frameworks, and then by complementing those with large fraud teams to help protect consumers from scams.

*Ms. DeGette. And do you think that the federal agencies have the necessary authorities to fight against these scams? Or can companies do it themselves? Do they have the authority to do it?

*Ms. Leggin. We value our partnerships with all the law enforcement entities, including the FCC, FTC --

*Ms. DeGette. Right. Do you think they have enough authority to do it?

*Ms. Leggin. We think --

*Ms. DeGette. Yes or no will work.

*Ms. Leggin. We think that the best authority, the best way for them to continue to help us, is by prioritizing resources towards enforcement.

*Ms. DeGette. Resources. So that means Congress and the administration have to adequately fund them, right?

*Ms. Leggin. We continue to work --

*Ms. DeGette. No, a yes or no will work.

*Ms. Leggin. Yes.

*Ms. DeGette. Okay. Mr. Winters, do you think they have enough authorities?

*Mr. Winters. No.

*Ms. DeGette. And why is that?

*Mr. Winters. I mean, if they did and they had the resources as well, I think we probably would not be here today. You know, they need an ability to, as I mentioned, follow up on the fines that they levy and actually collect those. They need sort of required transparency and basic moderation obligations for AI companies. There are lots of things that just using something like unfair deceptive practices authority are --

*Ms. DeGette. Okay, thanks. We look forward to working with you to see what new authorities we want.

*Mr. Winters. Definitely.

*Ms. DeGette. I just have a little time left, so I want to ask you one more question. In the bill, the great big bill a couple weeks ago that we are now learning all of the things that were included, one of the things that was included in the reconciliation package was a 10-year moratorium on state and local enforcement of their own AI bills.

Does a 10-year moratorium on state AI bills prevent states from using evolving technologies to help fight this program? And do you think that's something Congress should look at, Mr. Winters?

*Mr. Winters. So we vehemently oppose the moratorium provision. I do not think the moratorium as written would stop state agencies from using AI, but it would harm consumers without a doubt.

*Ms. DeGette. Thank you. I yield back.

*Mr. Balderson. Thank you.

Next up is my good friend Mr. Griffith from Virginia.

*Mr. Griffith. Let me start in a little bit different direction than I planned on going, Ms. Leggin. You were asked about adequate funding a minute ago, and I got the sense that while you were told to give a yes or no answer, you wanted to see the Federal Trade Commission and others to receive adequate funding. But it seemed to me that you were not trying to get into the debate as to what the definition of adequate funding is. Am I correct that I read your body language correctly? That you did not want to get into that debate, but you do want them to be adequately funded?

*Ms. Leggin. That is right. It is up to each agency to allocate resources to their enforcement teams. But what we have said, and what we are seeing with our work with our enforcement partners is that sometimes the consumer fraud protection folks lack the personnel or resources they need to go after cases. So we welcome, you know, information collection or just a way to try to allocate the existing resources --

*Mr. Griffith. But it is also true that AI may make this much more efficient, and so we are looking forward to that, too. Is that not correct?

*Ms. Leggin. That is right, AI --

*Mr. Griffith. I have to move on to what I was really going to go after. But for you and Mr. Bercu, the good news is that the fraud, while terrible, is on the downward slope. And I hear from my constituents all the time about receiving robocalls. And a couple of years ago, it was all about the fraudulent stuff and they were concerned about that. But I will tell you in the last year, particularly in the last few months, the real concern has become Medicare and particularly Medicare Advantage solicitors calling up the folks in my district. And I have an older population, generally speaking, than most districts. And they are just driving them crazy with all these calls.

And a 2023 survey estimated that 30 percent of Medicare Advantage eligible beneficiaries received seven or more calls a week.

I have to tell you, Mr. Chairman, and witnesses, I have had constituents who have told me if they only got seven a day, they would be thrilled. That would be a down number.

So what can we do? Because this is a huge issue in my district. What can we do to make that situation better?

*Mr. Bercu. Yeah, I think that those calls, if they are robocalls, if they are telemarketing calls, they may be in violation of the TCPA, they may be in violation of the telemarketing sales rules.

*Mr. Griffith. So how do we get them to use -- because I have asked. I have said to folks as I have been talking with them, have you put yourself on the do not call list? And they said, yes, but it does not seem to change anything. So how do we make that better?

*Mr. Bercu. I mean, so one of the things is, and we would be happy to work with you, we have got to trace back those calls. We have to see who is ignoring the law, get that information, get that to the right enforcement authorities to go after them. And we have seen success with that. Like the auto warranty campaign was the same. We worked very closely with the states and the FCC, and that went from the most prolific robocall campaign in America to basically zero right now. So that is the answer there.

*Mr. Griffith. All right, well, I will be glad to work with you in any way, because when I start going to events and I start hearing this at, you know, at a majority of the events I go to, whether it be a street festival or a meeting of folks, that tells me we have a problem.

Ms. Leggin, I got the toll texts. Of course, I called my staff assistant and said, how come you have not kept my account up to date.

[Laughter.]

*Mr. Griffith. Not realizing -- I was on the road. And she said, it is a scam, do not worry about it.

But I have gotten a number of those things since then, and some others. And apparently, somebody out there thinks I need a new job. And I click delete. I report as junk and delete. Does that do any good?

*Ms. Leggin. It certainly does. That is one of the key tools that the wireless industry and our partners on the device side have made available for consumers, to delete, report junk. You can also forward your scam texts to 7726, which spells "spam'' and both of those are key inputs for wireless providers and our messaging partners in making our algorithms and filtering and blocking more sophisticated and responsive to what we are hearing from consumers out there, like you and others in this room that have gotten those types of texts.

In addition, we look at those types of scams and we different evidence on them and refer them to our law enforcement partners through our secure messaging initiative as well, so that we are working to target the bad actors responsible.

*Mr. Griffith. All right, I appreciate that.

Mr. Waguespack -- and I hope I get your name right.

*Mr. Waguespack. That is pretty good.

*Mr. Griffith. All right, not too bad.

I do not know that I really have a question for you, but I will just make a comment. As a recovering attorney, I hate the whole strike suit industry, where they get an itch and they just go after things. I want people to be able to sue when they are legitimately harmed. And I just make the offer that if I can work with you in any way to try to make the law so that it lets the legitimate complaint go forward but stops the strike suits where they are just trying to make it expensive and get a settlement, you talked about that earlier, just let me know what I can do to be of assistance. I will try.

*Mr. Waguespack. I appreciate that. That is the balance we are looking for, and the balance is found in other federal statutes all across the Code.

*Mr. Griffith. All right, I appreciate it, and yield back.

*Mr. Balderson. Thank you, Mr. Griffith.

Next up is Mrs. Trahan.

*Mrs. Trahan. Thank you, Mr. Chairman.

Well, I am glad to know that the frustration of unwanted robocalls is as universal in Congress as it is with our constituents. According to one estimate, Massachusetts residents received over 43 million robocalls in the month of May alone. Each of these unwanted calls wastes the precious time of the people we represent, and there are real risks that the caller on the other end is a scammer looking to swindle them out of hundreds or even thousands of dollars.

The scourge of robocalls and robotexts must end. And yet the Trump Administration does seem determined to cut enforcement agencies like the FCC and the FTC who fight for Americans every single day.

Mr. Winters, can you just explain in brief the role that the FCC plays in combating robocalls and texts and how this agency works with private sector partners to do that?

*Mr. Winters. Sure, thanks for the question.

The FCC has a lot of responsibility and a big thing, you know, to cover. But one of the things they do is maintain and establish the robocall mitigation database. They have enforcement and investigation teams for, you know, reading consumer complaints, taking them in, analyzing it, and trying to do enforcement when possible. And I think they also, you know, work with industry colleagues, and maybe I will speak more to that, to try to ensure that they are doing as much as they can.

But I think already, even when there were no cuts to staffing, it is really hard for them to actually make meaningful consequences for the repeat bad actors, whether it is certain ability to get the fines themselves, or the fact that there is a relatively low standard for the robocall mitigation database. There are all sorts of reasons why, even if fully staffed, they do not have quite the right authorities or the right approach. And so, you know, to cut their staffing would make it even harder.

*Mrs. Trahan. Thank you. In February, President Trump signed the Executive Order 14215, incorrectly named Ensuring Accountability for All Agencies. This EO strips the independence from many of our regulatory agencies including the FCC. And the FCC is essential in the fight against illegal robocalls, making the actions of the Trump Administration all the more concerning.

Mr. Winters again, what effects will there be in the fight against illegal robocalls and texts if the Trump Administration undermines the independence of federal agencies like the FCC?

*Mr. Winters. Thanks. Yeah, the independent nature of the FCC and the FTC both is essential for them to be able to focus on consumer protection and not go down political pursuits. I highlighted a little bit in my oral and wrote more about it in my written testimony. But particularly at the FCC, this relationship with the White House has taken priority and makes it so Chairman Carr is most of the time talking about DEI hiring practices at companies and threatening to pull licenses for airing interviews with Democratic candidates, for example. As well as, you know, just focusing on, you know, providing contracts for people like Elon Musk in getting Spectrum lines.

All of that focus is not on consumer protection. Right? And one of the reasons why is because of that lack of independence where they cannot focus on that because they are sort of, you know, focusing on the priorities of the President.

*Mrs. Trahan. Thank you. The FCC's budget justification lists cracking down on illegal robocalls as a performance indicator for the agency, which is a necessary priority. Unfortunately, the Trump Administration has doubled down on its mission to hamstring the federal government's ability to hold robocall scammers accountable by proposing to eliminate 74 positions at the FCC in the Fiscal Year 2026 budget.

The FCC, however, is not alone in fighting robocalls. Industry has, in many instances, implemented solutions and voluntarily adopted best practices. Yes, they can always do more. But as lawmakers, we should look to build upon their good work while identifying gaps where the federal government can add value.

Ms. Leggin, can you discuss the importance of public-private partnerships in combating robocalls and robotexts, and suggest specific ways in which Congress can accelerate the efforts that industry has already taken?

*Ms. Leggin. Thank you. Public-private partnerships are a key tool in helping us go after bad actors so that we are stopping robocalls and robotexts at the source. CTIA's members participate in the USTelecom Industry Traceback Group to help identify the bad actors behind illegal robocalls, and our members on the wireless side, and then also throughout the messaging ecosystem participate in CTIA's secure messaging initiative, which convenes the messaging ecosystem to share information among each other and with our law enforcement partners across the federal agencies and with the state attorney general enforcement task force so that they can take that information and go after the bad actors as well.

*Mrs. Trahan. Thank you. Thank you to all the witnesses. I appreciate it.

*Mr. Balderson. Thank you.

Next up is the gentleman from Pennsylvania, Dr. Joyce.

*Mr. Joyce. Thank you, Chairman and Ranking Member, for holding today's hearing. And thank you for all of the witnesses who have agreed to testify today.

When I return to my district, Pennsylvania's 13th Congressional District, I hear about the pervasive and unrelenting illegal robocalls and texts that my constituents are faced with often on a daily basis. So many of my constituents are senior citizens. I sat down and did a senior citizen seminar twice in the district in the last month, and you hear recurrent themes. You hear the, "Grandma, grandma, it's Mike, I'm in Mexico and I'm in jail. I need your help. I need it.'' It sounded just like Mike. I hear that repeatedly when I have these roundtable discussions with seniors.

And it seems like the scammers are getting creative and finding actually new ways to trick us with incredible looking text messages and very convincing grandma and grandpa calls. Scammers have even learned how to incorporate AI into intimidating loved ones to convince them to turn over personal information. Credit card numbers, bank numbers. Too many of my constituents are risking their retirement savings, and subsequently they lose faith in the system that we have set in place to protect them.

We need to do better. We need to both educate consumers and anticipate the next angle of attack that these scammers will take, particularly with the assistance of our partners in law enforcement and the DOJ.

Mr. Bercu, your testimony mentioned a project piloted by the Industry Traceback Group, ITG, in partnership with banks and carriers aimed at tackling fraud and consumer financial losses. Can you elaborate on the pilot goals and successes thus far, and is there collaboration with law enforcement?

*Mr. Bercu. Yeah, absolutely. I think some of the most promising work our industry is doing is partnering across sectors, because the fraudsters are hurting our collective customers, whether that is banks or the carriers and your constituents.

So what we have been doing is working with banks to help them identify where their number has been spoofed, and a few carriers. So working with the carriers, getting examples of calls that the carriers see from the bank's number, getting that back to the bank, and the bank can tell us, oh, those were not us.

And what we are doing with that is two things. We are able to trace that back, find out who made the calls, find out who was spoofing the number, get that information in the hands of law enforcement to take action with it, but also help the bank identify and look at those customers and say, oh, did any of these customers that got the fake call pretending to be us have a suspicious transaction, and helping to find that. And I think criminal enforcement has to be key here, because that -- we know the scammers will use any tool available to them, and they will not stop just because it gets a little harder. They keep evolving. And so the key is going after them. And we stand ready to continue to support that.

*Mr. Joyce. And I agree, the scammers certainly have the ability to be incredibly crafty, devious, and downright evil in this regard.

Talk to me about how you interface with financial institutions to make them aware of these situations.

*Mr. Bercu. So I think that is actually one of the promising things going on across the industry, is that we work directly with a lot of the financial institutions, we work with tech companies, others. Marriott was mentioned before. We worked very closely with Marriott to trace the calls pretending to be Marriott. So that is what we are doing. But there are broader conversations now about how the industries can even keep growing and continue to integrate.

In my opening testimony, one thing I mentioned that I think Congress can do to help here is a safe harbor for that fraud information sharing, because I think there are questions about rules and risks when you do share information. So I think that is one way we can continue to lock those good partnerships.

*Mr. Joyce. And thank you. Thank you for being proactive in this.

Mr. Waguespack, many of my constituents are in rural central Pennsylvania, where internet connectivity is difficult and educational digital resources on illegal robocalls are inaccessible. How can federal agencies and industry partner, coordinate efforts to better educate consumers specifically in rural areas with limited internet access in those digital resources?

*Mr. Waguespack. Well, I think on leaning into what has been done since TCPA was first initiated, where you have private sector solutions going in and working with -- we have talked a lot about FCC and FTC, but also the local law enforcement and local financial institutions on the ground there, putting that initiative out there.

Mr. Bercu talked about some of the information sharing that is done with the banks to prevent the fraud. There is also a second level down that is a good example of the education program. Through the bankers association, they have armed about 2,000 banks out there to talk to their consumers, here is a hit list of the things we will never ask you for, so if you get an email that has this, this, this, or this, ignore it, it is spam, here is how you call us back. And so we can use the private sector, I think, to develop some of that messaging and make sure consumers can be informed with the decisions they need to be able to fight back on their own.

*Mr. Joyce. I thank all of the witnesses for presenting here today. Mr. Chairman, my time has expired and I yield back.

*Mr. Balderson. Thank you.

Next up is the gentlelady from Texas, Mrs. Fletcher.

*Mrs. Fletcher. Thank you. And thanks to our Chairman Palmer and Ranking Member Clarke for convening this hearing today. Thank you to our witnesses for all of your testimony. I think it has been really helpful for all of us. And as we have heard throughout the morning, abusive robocalls and robotexts are not just nuisance, right? They are a danger. And we need to do something about that.

I appreciate the work that you are doing, and also the issues that you have brought to our attention this morning, and the conversation around what we can do about it.

You know, I am concerned, as several of my colleagues have mentioned, that we are hearing consistently from you we need more enforcement, we need more coordination, we need adequate resourcing, and we need adequate staffing to be able to do some of the things we are doing in a complex and challenging environment where the technology is moving faster than Congress, faster than our agencies. And what we are seeing at the same time is that those resources both in terms of money and staff are being cut from the administration. As we speak, they are asking Congress to rescind additional funding. They are stopping funding.

And so, you know, as several of my colleagues have noted, agencies like the FCC, the FTC, and the DOJ have actually utilized the law that we passed together, the work that we have done collaboratively, to und the problems and really conduct meaningful enforcement that has stopped scammers. And now, it seems like the administration is taking the cops off the beat in this area and in many others.

Mr. Winters, you noted in your testimony and you mentioned just earlier this morning that the Trump Administration has taken steps to dissolve the DOJ's consumer protection bureau. And I believe you just said the consumer protection branch of the DOJ, you just told us this morning that they had successfully prosecuted a case and stopped scammers who had -- I guess it was against the data brokers who had sold the data of 30 million Americans. And that data winds up in the hands of criminals who use it in these scams and others. So I think it's really important that we und that these agencies need to be fully funded and that shuttering something like the DOJ's consumer protection branch, this expert-led enforcement agency, really puts our communities at more risk. It is not something we should be doing.

You also mentioned in your testimony that the CFPB, the Consumer Financial Protection Bureau, and the work that it has done in this area, and the administration is also shuttering or attempting to shutter that agency that Congress created and that has been really critical to protecting consumers. And that's what we're talking about in this hearing, protecting consumers, protecting American citizens from these scams.

I think that what we are hearing this morning also calls on all of us on this committee to redouble our efforts to do our work around creating comprehensive privacy laws that protect American consumers. Because what I am hearing from you and what we are seeing is that our data is being stolen, is being sold, is being used. And it is being used by these scammers.

So can you take, with the time that we have, just can you talk a little bit more about cutting the DOJ's consumer protection branch as well as the CFPB, and what that would mean, Mr. Winters, in terms of protecting American consumers? In this larger context, if you want to talk too about the effort to take away the staff and the funding for these agencies that are protecting consumers from robocalls and robotexts that we are all clearly worried about and clearly concerned. We want to address how is this going to help or hurt us in that effort.

*Mr. Winters. Yeah, absolutely, and thank you for the question. I mean, very simply, taking resources away from these agencies, and in the case of the CFPB and this part of the DOJ, completely trying to stop all of their work is absolutely not going to help in the fight against these harms.

On the DOJ consumer protection case that I mentioned, yeah, that is a data broker that sold a list of over 30 million elderly Americans directly to a scammer. It is not just that it ended up in the scammer's hands. Data brokers will sell to anyone at any time. And so what Congress needs to do for both scam reasons and lots of other reasons, is pass comprehensive data privacy law with data minimization and a private right of action and a few other key things. Or at least, if you want to be more focused, it should be focused on restricting the sale of consumer data.

CFPB specifically, shuttering that really cuts off a central resource for people that are victims of scams, especially. They have had, you know, counselors, people that answer the phone and take complaints and try to get things resolved for you. There are a bunch of great stories of people that literally had their scams resolved. You know, they got money back from their bank with the help of CFPB professionals. So they can do things on enforcement and work with financial actors where people are losing their money. But they also are just critical support. And they provide also tracking of those complaints and, you know, gets it to state AGs and those who can help.

*Mrs. Fletcher. Thank you, Mr. Winters. I have gone over my time. I do have more questions for the panel, so I will submit them for the record, and I will yield back. Thank you.

*Mr. Balderson. Thank you.

Next up is Mr. Tonko.

*Mr. Tonko. Thank you, Mr. Chair.

Americans received over 52 billion robocalls in 2024, which is nearly 200 calls for every American adult. Americans also have lost 25 billion annually to scams that begin as spam calls. Unfortunately, we know the scammers often target older Americans who are especially vulnerable victims to these scams. Older adults in particular lost 4.9 billion through all types of fraud last year alone.

I know I listened to the exchange that you had with my colleague, Representative DeGette. But I want to delve into this with the senior perspective.

Certain scams put even the most technically savvy at risk, scams that in some cases mimic law enforcement, hospitals, or Medicare, or the voices of family members seeming to be in danger or in need of money.

So, Mr. Winters, what specific tactics do scammers use to target seniors and other vulnerable groups?

*Mr. Winters. Yeah, I mean, and thank you for the question. Scammers in general capitalize on uncertainty and fear. And especially for seniors, especially those who are on a fixed income, all sorts of concerns about an unpaid bill, a toll account that you do not quite have set up yet, Medicare, you know, potential fraud and targeting, like they are going to be thinking that the senior citizens are good targets for it. This is exactly why we had the case where a data broker bought a large list of senior citizens and targeted them with scams. And that is, you know, a terrible thing.

And so, again, yeah, they try to capitalize on uncertainty and fear. And that is why you see lost bills, job opportunities, especially in this current climate where a lot of people are getting fired and the economic uncertainty is everywhere, the job opportunity scams are going to be -- more people are going to fall for them because, you know, you want a job, you need a job, you need to pay your bills.

So, you know, I think that those are some of the ways in which they are targeting everyone. But, you know, are hitting seniors most.

*Mr. Tonko. And what prevention strategies have been the most successful in that fight against illegal robocalls and texts?

*Mr. Winters. Yeah, so, you know, there have been really strong enforcement actions by the Federal Trade Commission of voice-over-internet providers. So, you know, I think the most appropriate and effective enforcement is going sort of upstream, especially when you are trying to get accountability for some of the actors that are providing the content or the delivery or the targets of some of these scams.

One other really good case was the Rytr case by the FTC last year, where they targeted using the means and instrumentalities concept. In this case, it was a tool that generated lots of fake reviews, and the FTC was cracking down on fake reviews. But you can use that same tool to generate sort of an endless list of scam texts. And that sort of, you know, is a force multiplier for scammers.

And again, you know, the use of these AI tools makes it harder because, you know, there are no typos. It comes in, you know, perfect English. And there's no, you know, these weird links that we have all sort of become accustomed to, so that makes it even tougher.

*Mr. Tonko. Thank you. And, Ms. Leggin, how is the wireless industry working to protect that older community and otherwise more vulnerable customers?

*Ms. Leggin. That is a priority for the wireless industry. And to do that, we work with AARP and we support their National Elder Fraud Coordination Center, which works to take reports of victim losses in and then bring cases against bad actors.

We also were happy to participate in the FTC's Stop Senior Scams Working Group, and we led the working group focused on text messaging issues, which was a cross-sector effort to explore ways that we could do more to protect older Americans from scams.

We also participate in other working groups with consumers directly to try to push out our educational materials so that they know which text not to click on, which calls not to answer. And we have those resources on our website and our members' websites as well.

*Mr. Tonko. Thank you. And the AARP that you mentioned has said that, and I quote, "The alarmingly high levels of fraud against older adults underscores that stronger protections are urgently needed.''

So as technology evolves, so must our ability to combat these illegal and harmful calls and texts. Mr. Bercu, what additional tools does the Industry Traceback Group need to protect Americans from fraudulent calls or fraudulent texts?

*Mr. Bercu. Thank you for the question. So I mentioned in my opening testimony I think there are ways to build on what is working and reinvest in our work. We are always adapting to the threat. A few years ago, we were only really tracing illegal robocalls. Now we are tracing threatening calls, we are tracing targeted scams. And I think that doubled last year how many we traced. So we are always adapting and I think Congress's support through targeted immunity, through extending the cycle, will allow us to continue to invest and to innovate.

*Mr. Tonko. Well, I thank you very much.

And with that, I yield back.

*Mr. Balderson. Thank you.

Next up is the gentlelady from New York, Ocasio-Cortez, please.

*Ms. Ocasio-Cortez. Thank you, Mr. Chair.

Mr. Winters, I want folks back home to kind of understand why this problem is happening. You know, the average American receives about 15 robocalls each month, but obviously, depending on who you are, you could be experiencing that in a day. And we know that it was not always like this. So I want folks to understand what the root of this problem is, so that they also understand what some of our solutions can be.

Is it fair to say that essentially back in the day, calls used to be routed through phone wires, through your telecom company, and so your telecom provider, whether it was Verizon or AT&T or Tmobile, they were responsible for routing the calls and therefore they were kind of able to trace who was making them; is that right?

*Mr. Winters. Yes.

*Ms. Ocasio-Cortez. And then, as internet applications started to grow, then voice service providers and calls over digital services started to really expand in their infrastructure. And so it was not just your cell phone provider or even your landline provider that was in charge of your phone calls, it then became kind of these other kind of internet companies, right?

*Mr. Winters. Yeah, there are a lot of intermediary service providers. Sometimes a call will go through like eight or 10 of them before reaching you through AT&T or whatever.

*Ms. Ocasio-Cortez. Yeah, so it was really in that switch from call and telecom providers to the expanding growth of internet providers that really kind of allowed the volume of these calls to blossom, because we were not just talking about telecom regulation, but internet regulation, right?

*Mr. Winters. I think that's definitely a lot of the reason to blame for those additional intermediary providers that are harder to track through.

*Ms. Ocasio-Cortez. And so it is no longer about who your personal provider is, as you said, you could have eight, you could have 10 of these companies routing this call. So you have the person who wants to make this robocall, and then it just leapfrogs between all these intermediary companies. Mr. Winters, how many of these intermediary companies currently exist? And does the government have any way to keep track of who these actors are?

*Mr. Winters. Thanks for the question. Yeah. It is kind of an unanswerable question. I think since we have been there, there are probably additional companies that have popped up and registered on the robocall mitigation database. I think last time I checked a few days ago, it was over 9,500 of these intermediary service providers. And so, you know, there is a list online. It is not a high barrier to entry. You have to, you know, register that you are a company, you have to put a robocall mitigation plan in the form. But there is not a lot of vetting there. Right?

*Ms. Ocasio-Cortez. And if these kind of abusive companies -- sure, they have to register. But if we find that they are not complying, the consequence just seems to be that they get delisted from the database, correct?

*Mr. Winters. Only sometimes. Not even that sometimes.

*Ms. Ocasio-Cortez. Okay. But without any additional penalties, is there anything to stop these companies from just immediately getting relisted?

*Mr. Winters. No. You can, you know, if you are delisted, you can get another corporation and set it up and sign up again.

*Ms. Ocasio-Cortez. So if you are a bad actor in this space, someone that is, you know, really perpetuating spam calls, in some cases fraudulent calls, you can be found to be breaking these rules, you can get delisted from the FCC, and then you can just turn around and it is, what a hundred bucks to --

*Mr. Winters. I think that is not even necessarily in force, yet. But, yeah, it will be a hundred bucks.

*Ms. Ocasio-Cortez. Yeah, it's a hundred bucks and maybe you will have to pay it, maybe not.

*Mr. Winters. Um-humm.

*Ms. Ocasio-Cortez. So clearly, there is an enforcement problem here in keeping these bad actors out of the space.

In your opinion, as a consumer protection advocate, how can we as Congress work to strengthen some of these protections? And what do you think some of the best solutions here are?

*Mr. Winters. Yeah, I think particularly to the lack of accountability in the robocall mitigation database, you know, there are a few really easy things that either the FCC can do or Congress can instruct the FCC to do to speed that up, I guess. There is a really low barrier. Right now, you have to have reasonable precautions of taking -- you know, to mitigate robocalls. And that standard should be increased to effective, actual implementation. There should be requirements for the downstream providers, the bigger companies, to have responsibility for the calls that they are taking in from those eight to 10, whatever, plus intermediary service providers. And, you know, there is just insufficient tracking, insufficient consequences for repeat offenders, even. Even under the company they are doing.

And one thing we advocate for to try to increase that accountability, because it is genuinely a difficult problem to try to track all these service providers, even if there is a full-court press. But one proposal we have put out there is to implement bonding for robocall mitigation database members, so that a third party is incentivized to make sure that they are actually doing what they say they are going to do and help protect consumers. So very happy to work with your office to try to make that happen. Thanks.

*Ms. Ocasio-Cortez. Thank you very much. I yield back.

*Mr. Balderson. Thank you.

Next up is Mr. Mullin for five minutes.

*Mr. Mullin. Thank you, Mr. Chair. Thank you all for being here today.

Americans lose billions of dollars every year to phone-based scams. We must crack down on illegal robocalls and robotexts.

With the recent enactment of laws that further empower enforcement agencies, there has been progress toward protecting people from these predatory practices, but not enough.

I want to recognize former Congresswoman Anna Eshoo, who represents a district neighboring mine. She has represented that for over 30 years before her recent retirement. I want to thank her for her leadership on this issue.

She introduced key legislation like the Hangup Act and the Robocalls and Texts Act, and I am proud to help uplift some of that work that she led on in this committee and hopefully carry it forward in the future.

As we have heard today, more must be done to keep up with the rapidly advancing technology and the increasingly sophisticated tactics that scammers are using. Enforcement agencies need the tools and resources to stay ahead. The more sophisticated the methods, the more likely people fall victim to them. As more companies integrate AI into their products, it is becoming even harder for consumers to distinguish legitimate communication from fraud.

Mr. Bercu, you mentioned AI generated messages are harder to detect and can present challenges for enforcement. How can the government and industry better coordinate to establish safeguards to limit harm to people from illegal calls using AI?

*Mr. Bercu. Thank you for the question. I think it -- the fact that the criminal actors behind these calls use AI just underscores they will use every tool, every channel available to them to defraud Americans. And I think that is one of the challenges we have, is they are not going -- they are already violating the law with impunity. They are committing fraud, that is violation of the criminal code. So that is one of the things I think we think, is we do need a national strategy. We do need to prioritize criminal enforcement, because they are going to continue to use the tools. And from the carrier perspective, there is not going to be a good way to know which tools they are using because, as Mr. Winters pointed out, they are so far upstream from where our members sit.

*Mr. Mullin. Thank you for that. We know that certain people in our communities are particularly vulnerable, like seniors and individuals with limited English proficiency. Mr. Winters, what can the FTC in coordination with other agencies do to be proactive in protecting vulnerable populations from these kinds of scams?

*Mr. Winters. Thank you for the question. You know, I think it is a lot of the same, of working to cut off the problem at the source. Right? So whether we are talking about an AI tool that makes it super easy to generate a million texts that threaten to be immigration enforcement or something, for example. The enforcement action should target those developers that are putting those products out there.

Same thing goes for, you know, putting liability and responsibility for people throughout the call stream, to make sure that the calls they are taking content from are, you know, actually doing what they're saying they're going to do.

But I think that the FTC and all these, you know, state attorneys general as well can be doing more to do better investigation of the members of the robocall mitigation database, making sure that the STIR/SHAKEN protocols are implemented, you know, thoroughly and it actually does what it is supposed to do. I think a lot of times, we see scam calls that have the high level of attestation, despite that being the whole point. So I think that there is just a lot more that they can do together.

*Mr. Mullin. And you also strongly assert, Mr. Winters, in your testimony that the FTC's overall enforcement capacity has been diminished by the recent unlawful firings of two Democratic commissioners, and deep staff and budget cuts at the agency. So how are those agency cuts going to hinder FTC's ability to advance its efforts to combat illegal robocalls and robotexts?

*Mr. Winters. It will hurt their ability to do so. As we have talked about, it is already a really difficult issue, even if you are trying your best and have all the resources you can. If you are taking people away, especially at an agency like the FTC that has a really broad jurisdiction, of course you are going to have less resources, less creative cases, just because, you know, more things are being put on less people and the priorities are not there, either. And so especially without the commissioners, two of the five commissioners, you do not get dissent, you don't get the conversations that might generate more creative ideas or different ideas. And so between that and the staffing, it will just make it a lot harder.

*Mr. Mullin. Thank you for that. I yield back.

*Mr. Balderson. Thank you. Next up is the gentleman from Texas, Mr. Pfluger.

*Mr. Pfluger. Thank you, Mr. Chairman. Thanks for the witnesses being here.

I want to take a little bit different approach on this and just talk about a little bit of the impact that I am not sure has been fully discussed today, and that is to physicians. And in the process of getting screenshots of the physicians in my district, and one in particular who is showing me kind of the impact of about 20 a day that they are getting, that is really preventing -- these calls, these robocalls are preventing that physician from being able to take calls from the ER or from labor and delivery. And it is pretty concerning.

So apparently, the apps that they are using to either diagnose or have conversations with their patients, the Abridge app is one of them, and then there is another app, and I am not familiar with these, so I am not the expert on this. But you cannot use those apps when calls are coming in.

And so I just wrote down from the screenshot the calls that recently came in. This was from last week on Friday. 2:31, 2:53, 2:57, 3:48, 3:53, 3:58, 3:59, 4:38, and 4:48. And in that period of time, starting at 2:30, ending at almost 5:00 p.m., you know, there were a number of patients that were disrupted.

So I know we are beating a dead horse with just how painful these things are. But that actually is pretty serious, you know, when they cannot take a call from the labor and delivery section saying, hey, we have an incident here that you need to get up pretty quick and, you know, deliver.

So I will start with Ms. Leggin. And, by the way, thank you all. I know we are all working together to try to solve these. But, you know, to what extent do you see TCPA and TRACED being effective? And then I will go a step further. I mean, we have had these discussions already in this hearing. But, you know, the sense of urgency and what else needs to be done to prevent that physician and all the other physicians from having to deal with that in the middle of what could be an emergency situation?

*Ms. Leggin. Thank you for the question. And that seems like a serious issue.

TRACED and the TCPA are great tools that are helpful and helping bring enforcement actions against bad actors under the TCPA if you are violating those consent, auto-dialer, pre-recorded voice provisions. But unfortunately, bad actors do not care about the TCPA or other laws, so they are going to spam you no matter what. And that is where our work with law enforcement partnerships on the calling side through the ITG or on the texting side through the secure messaging initiative to bring investigations against those bad actors so that we are stopping those at the source are really helpful.

*Mr. Pfluger. Yeah, go ahead.

*Ms. Leggin. And I was just going to say you have heard me say throughout this hearing, we would welcome help from Congress in prioritizing resources towards enforcement to bring more cases against those bad actors.

*Mr. Pfluger. What do you think we can do, and anybody is open to answer this, what do you think we can do for hospitals in general? You know, for those that are providing emergency services. Because nobody is using a pager anymore. It is all cell phone. Maybe they need to go back to that.

But what can we do to think creatively to really stop that for those -- I mean, every constituent of mine wants it stopped. But are there specific ideas?

*Ms. Leggin. That is a good question. You know, it is a really challenging issue, especially when we want to make sure that critical public safety, public health services need to get their calls through. You know, the same tools that w apply to protect consumers can protect, you know, the personal lines of physicians and other things. Call blocking, call labeling, call filtering services. And then combining that with enforcement so that we are stopping those at the source.

*Mr. Pfluger. This particular physician goes through, deletes and, you know, reports junk and does -- reports it and does all that. So it sounds like it has been a continued issue.

I will go to Mr. Bercu. When we look at the gaps, and just kind of building on this same theme, you know, are there specific things that you would have us do to address those gaps and, if so, maybe describe how they affect, let's just go with the physician sector, health care.

*Mr. Bercu. Yeah, absolutely. And I think, by the way, I think we have the right framework. Mr. Winters was talking about the robocall mitigation database, and I could not agree more, we need to find ways to quickly find the bad actors in that database, get them out. The FCC does require that providers have to do due diligence about who they take traffic from. So we are developing the data to see who keeps taking traffic from these shell companies. So I am optimistic we will continue to make progress.

There are, as Ms. Leggin mentioned, there are blocking, labeling, and specific use cases. I know we work sometimes with some companies that sit on the inbound call side for a hospital. And we have had successful, and they have really sophisticated tools to see which is the consumer and which is not. So those are some of the things I would recommend that the doctor looks into.

*Mr. Pfluger. Thank you. My time has expired. I yield back.

*Mr. Balderson. Thank you.

Next up is Mr. Allen for five minutes, please.

*Mr. Allen. I want to thank Chairman Palmer for convening this hearing. And you probably heard this today from every district in the country, but my constituents frequently express their frustration with the persistent barrage of illegal robocalls, robotexts. They are a nuisance and they are a significant distress, anxiety, particularly for our elderly population, because some of these folks are up to no good, and are taking advantage of our constituents.

These communications often exploit our most vulnerable individuals. And it is really eroding our trust in the telecommunications systems. I look forward to receiving updates on the progress made under existing laws and exploring actionable next steps to protect consumers and strengthen enforcement. And I want to thank our witnesses for being here with us.

Mr. Bercu and Ms. Leggin, there has been a lot of public and private action in the fight against illegal robocalls, both under the Telephone Consumer Protection Act, and under the TRACED Act. Generally, robocall numbers have been on a downward trend over the years.

If illegal robocalls trends have dropped, why am I still getting so many complaints from my constituents?

*Mr. Bercu. Yeah, I think some of the members sort of expressed that. There are really positive numbers, the 50 percent reduction in scam robocalls. But not everyone is having the same experience. Some people do get more than others. So that is an ongoing challenge.

But there again, I think we have the right framework. We are tracing back those illegal calls. Some of those are illegal telemarketing. We are tracing them back. That information is making its way to enforcement.

And in terms of the scam calls in particular, we know that they are going to keep going. Just because it gets a little harder does not mean they say, okay, we are going to go do another line of business. They are just going to keep coming through a new channel, through a new method, through a new shell company. And so that is really where we think the answer has to be actually going after them with criminal enforcement. And we think that should be a priority.

*Mr. Allen. Ms. Leggin, would you care to add to that?

*Ms. Leggin. I agree with what Mr. Bercu said. You know, the framework that we have in place continues to show progress and we continue to build upon that with new tools and enhance those tools with machine learning and AI and the latest technologies to make them even better. And I agree that more focus on enforcement by taking those bad actors off the field is where we need help.

We saw a group of state attorneys general, for example, recently get a judgment against prolific robocaller Jonathan Spiller, so that that prevents him from starting new businesses or otherwise kind of popping up again after getting an enforcement action against him.

So things like that will continue to help make a big difference and continue to drive those robocall numbers down.

*Mr. Allen. So we are identifying these bad actors. It is just a matter of prosecuting them?

*Mr. Bercu. In many cases we are, where we are getting good data that can further the investigation. It is one of the reasons that I am actually optimistic about continuing to work across sectors, because we can now combine some of our data with some data that the banks can get that through, as Ms. Leggin mentioned, the AARP's National Elder Coordination Council. Really aggregate data. Because that is one of the challenges. If it is one scam, it is hard to get a prosecutor involved. But if you can show it is a multimillion dollar scam, you can. So that is still where some of the work needs to go.

*Mr. Allen. Well, thank you.

Mr. Waguespack, in April 2025, FCC issued a notice of proposed rulemaking. They proposed a two-year time line for providers to maintain non-IP infrastructure to either complete their IP transitions or fully implement one or more of the available non-IP caller ID authentication frameworks in their non-IP network.

In your opinion, is the FCC's two-year time line reasonable?

*Mr. Waguespack. I would yield to my colleagues to the right on more of the technical time line there, because they are the ones that are going to be implementing some of that.

I would say from our perspective, if I could just -- since I have the mic for a second -- bring in another universe of recipient of a lot of these robocalls that we have not really addressed yet. Is what lies in between business and consumers a lot of times is small business. Because a lot of those recipients, they are kind of part consumer, part business owner. Their cell phone becomes their business phone and their residential phone, et cetera. They cannot qualify for do not call if it is considered business or not.

That is a vulnerability that we hear a lot from our members on small business. And it is also a vulnerability that is being exploited from some of these predatory lawsuits I mentioned earlier in my opening statement.

*Mr. Allen. All right, you have answered my second question there about the impact, particularly in rural areas, and other non-IP networks.

Ms. Leggin, in your testimony, you discuss how CTIA and its wireless partners embark on the next generation of call identification solutions, namely branded calling. What is branded calling and how will it help reduce scams and scam calls?

*Ms. Leggin. Thank you for the question. CTIA is building the next generation of branded calling by bring together the wireless ecosystem players to give the consumer more information about who is calling and why. And branded calling, as the name suggests, means that the logo of the caller comes through.

This framework provides verified identity of the caller and builds upon the STIR/SHAKEN framework to make that information that comes through to the caller even clearer and better. So by doing so, we help empower the consumer to make better choices about do you want to answer the call or not. And we think that will be a really helpful tool in continuing to protect consumers from scam calls.

*Mr. Allen. Good. I thank all of you. And, Mr.

Chairman, I yield back.

*Mr. Balderson. Thank you. I now recognize the Ranking Member Clarke.

*Ms. Clarke. Thank you, Mr. Chairman. Mr. Chairman, I have a request for unanimous consent. Representative Sorensen sent a letter to the Chair and myself about the importance of taking action, and his bipartisan QUIET Act, which addresses some of the issues raised here today.

I ask for unanimous consent for his letter to be entered into the record.

*Mr. Balderson. We received the letter. And seeing no objection, accept it.

[The information follows:]

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

*Mr. Balderson. Thank you.

*Ms. Clarke. Thank you.

*Mr. Balderson. Next up, the gentleman from the great state of Ohio, Mr. Rulli, for five minutes.

*Mr. Rulli. Thank you, Chairman.

The question will be directed at Ms. Leggin. This is a bipartisan issue and I think the most engaging, sensitive constituency that we have, I would say over 60. When I was young, I used to listen to a lot of talk radio in the 1980s and the 1990s. And it was a subject then and it is just a subject as much right now today. They want to enjoy their peace and their tranquility. And these robocalls just keep ruining it.

So what percentage of illegal robocalls and spam text messages originate abroad? And where do they primarily originate from? What part of the world?

*Ms. Leggin. Thank you for the question. It is a mix of robocalls and robotexts that come from both the U.S. --

*Mr. Balderson. Ms. Leggin, your mic, please. Sorry.

*Ms. Leggin. Sorry. Microphone.

It is a mix. It comes from bad actors that are both located in the U.S. and outside the U.S. And we take seriously our work to protect consumers from illegal robocalls and robotexts that originate abroad. It continues to evolve. But southeast Asia is one area, including India and the call centers there that Mr. Bercu mentioned earlier continues to be a source of illegal and unwanted robocalls and robotexts.

So we support efforts like those at the FCC, where they have memorandums of understanding with international partners, with states to collaborate on enforcement against the bad actors located outside of the U.S.

*Mr. Rulli. Out of curiosity, do you think that America has migrated into an evolution where we have gotten better than we have in the early 1990s? Or not really?

*Ms. Leggin. We have definitely gotten a lot better than the early 1990s. And especially over the last 10 years on the robocall front, we have had a lot of attention to this issue from this committee, through the TRACED Act, from the FCC and other agencies giving us more tools, more authority to go after bad actors in this space. And there has been a lot of innovation in the texting space as well over the years to make our onboarding, our filtering, our blocking and consumer reporting tools even better. And we continue to enhance those very day.

*Mr. Rulli. Thank you so much. And then I have a question for Mr. Bercu. To fight against robocalls and spam texts, the FCC has formed international alliances and partnerships with countries like Australia, Brazil, Canada, the EU, Romania, Singapore, just to name a few. How should we move forward with helping the FCC handle enforcement with countries that are bad players, like in Laos and in Cambodia, who seem not wanting to get involved in the government? How can we get more involved with these countries that are allowing these illegal procedures to happen?

*Mr. Bercu. That is a great question.

*Mr. Balderson. Is your mic on?

*Mr. Bercu. Sorry. That's a great question.

So I think one of the things we would love to see is that is why we do need a national strategy, because the same people attacking us here are also attacking consumers in Canada and the U.K. and Thailand.

I think as we go around the world, there is more of a coalition of the willing to go after the criminal actors here. And so, you know, the FCC has those MOUs with other countries. But we also need it coming from the criminal law enforcement authorities at that level, and working together to take down some of these entities. And organized crime, really, is what we are going after with those.

*Mr. Rulli. Do you think it is obtainable?

*Mr. Bercu. I think it is obtainable. I think we have seen some other countries take very aggressive actions. For example, Myanmar is now building out their reporting about these fraud centers in Myanmar. The Thai government shut off the power. So they are going to generators. But I think there is room to continue to build on those and build those collaborations. Because again, those same entities are attacking us all over the world.

*Mr. Rulli. Outstanding. Thank you so much.

And with that, I yield my time back to the chair.

*Mr. Balderson. Thank you. Next up is the gentleman from Texas for five minutes, Mr. Weber.

*Mr. Weber. Thank you, Mr. Chairman.

Ms. Leggin, I am coming to you. I had to be at another hearing for a long time. I apologize if this is redundant.

In many cases, robocalls are so believable that millions of Americans fall prey to the various scams every year. However, the recent rise in robotexts as we call them adds a new layer of complexity. What makes combating spam and scam texts, why is that more difficult than robocalls?

*Ms. Leggin. Thank you for the question. CTIA and our members throughout the messaging ecosystem take seriously our goal to protect consumers from illegal and unwanted robotexts. Voice and text are different technologies and they present different ways that bad actors target consumers. So we've got different problems with different solutions.

So it is just a different ecosystem where we still bring blocking tools to bear in the texting space. For example, we blocked over 55 billion scam texts just last year. But that is just one piece of the --

*Mr. Weber. Can I give you my cell phone and have you block some more?

[Laughter.]

*Ms. Leggin. Happy to help, yes.

We continue to up those efforts and bring new tools to bear.

In messaging, we've got tools throughout the message flow, including up-front vetting and verification services that help identify whether legitimate businesses are who they say they are. And it helps deter bad actors from getting on the platform in the first place. We've got sophisticated algorithms, machine learning, AI, and fraud teams that look at ways to protect consumers from unwanted and illegal text messages in the middle, and then we've got consumer reporting on the back end so that you can delete and report junk, or you can forward your spam text to 7726. And the wireless industry takes those in to use to enhance our protection tools so that we are taking in that consumer feedback to make those tools even stronger.

*Mr. Weber. Do you know, this question may be a little bit to the left, do you know or are you all able to determine how many texts a company sends out at any given time? They send out a million, 10 million? Can you identify that, know that?

*Ms. Leggin. So companies use a variety of different platforms to send out their communications. So to us, that is not something that we look at. What we look at is trying to make sure that we are looking for suspicious patterns, indicators of spam or other illegal things to target those to protect consumers from those. Otherwise, it's really a balance to protect consumers while also making sure that legitimate business communications go through.

So like I said, we blocked 55 billion last year. But we also let -- you know, supported 2 trillion texts to go through. So it is always a balance.

*Mr. Weber. Well, I think a trillion of those came to my cell phone.

Mr. Bercu, I am going to come to you. As you are probably aware, there are varying levels of jurisdiction and oversight when dealing with either foreign or domestic entities.

Now, I missed the first half of his question. So if this is redundant -- did he ask you about this?

*Mr. Bercu. He may have but I am happy to --

*Mr. Weber. Well, what are some of the unique challenges regulators and law enforcement face when dealing with foreign originating robocalls? Is that what you all just went through?

*Mr. Bercu. We went through an aspect of that. But I am happy to talk about it. We have traced -- in our tracebacks, we have traced calls --

*Mr. Weber. And how do they vary from domestic ones?

*Mr. Bercu. Yeah. So I think in our experience, both one what we have seen through our tracebacks but also some public reporting, I think what we see is that illegal telemarketing, often that is homegrown and there are entities -- John Spiller, Ms. Leggin mentioned earlier. That might be more local. But we do see a lot of the fraud comes from abroad, especially the scaled fraud.

So in terms of other countries, I think those same actors are attacking everyone around the world. I think there is a lot of work to be done collaboratively with other countries. We have traced those. We do trace those. We find those entities. We sometimes see entities log into our portal saying they are a U.S. company but log in from abroad. So I think we are building that dataset and it can arm criminal law enforcement to go after it.

*Mr. Weber. Okay. Very quickly, our first responders, medical professionals, and others often deal with individuals who are at their most vulnerable, making them a prime target for potential scams and attacks. So the question is going to be, but I have one to ask real quick, how do we address spoofing related to hospitals, police, government agencies, and other public service entities? And I want to hone in on this as a question for the two of you all. And we will go back to you, Ms. Leggin. How about have you all ever encountered what is known as swatting?

*Ms. Leggin. Yes.

*Mr. Weber. And how often? Or would you put a percentage on that? And what do you do about it?

*Ms. Leggin. So we take swatting very seriously. You know, that is where someone calls in a fake emergency and has, you know, a police team go to your house. That is something where we are not really seeing that as much on wireless 911 calls as much as it is on other networks. But regardless, the same tools that protect consumers from illegal and unwanted robocalls, like call authentication, like STIR/SHAKEN, call filtering, call blocking, and then tracing back calls after they have gone through to find the bad actor responsible are all things that we encourage to address swatting, as well as partnerships with law enforcement to go after that criminal activity as well.

*Mr. Weber. Okay. I thank you, Mr. Chairman. I yield back.

*Mr. Balderson. Thank you. Seeing no other members here wishing to ask questions, I would like to thank our witnesses again for being here today. Without objection, that will be the order.

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

Without objection, the subcommittee is adjourned.

[Whereupon, at 12:24 p.m., the subcommittee was adjourned.]