

**RINGING OFF THE HOOK:  
EXAMINING THE PROLIFERATION  
OF UNWANTED CALLS**

---

**HEARING**  
BEFORE THE  
**SPECIAL COMMITTEE ON AGING**  
**UNITED STATES SENATE**  
ONE HUNDRED FOURTEENTH CONGRESS

FIRST SESSION

WASHINGTON, DC

JUNE 10, 2015

**Serial No. 114-07**

Printed for the use of the Special Committee on Aging



Available via the World Wide Web: <http://www.govinfo.gov>

U.S. GOVERNMENT PUBLISHING OFFICE

SPECIAL COMMITTEE ON AGING

SUSAN M. COLLINS, Maine, *Chairman*

ORRIN G. HATCH, Utah  
MARK KIRK, Illinois  
JEFF FLAKE, Arizona  
TIM SCOTT, South Carolina  
BOB CORKER, Tennessee  
DEAN HELLER, Nevada  
TOM COTTON, Arkansas  
DAVID PERDUE, Georgia  
THOM TILLIS, North Carolina  
BEN SASSE, Nebraska

CLAIRE McCASKILL, Missouri  
BILL NELSON, Florida  
ROBERT P. CASEY, JR., Pennsylvania  
SHELDON WHITEHOUSE, Rhode Island  
KIRSTEN E. GILLIBRAND, New York  
RICHARD BLUMENTHAL, Connecticut  
JOE DONNELLY, Indiana  
ELIZABETH WARREN, Massachusetts  
TIM KAINE, Virginia

---

PRISCILLA HANLEY, *Majority Staff Director*  
DERRON PARKS, *Minority Staff Director*

# C O N T E N T S

---

	Page
Opening Statement of Senator Susan M. Collins, Chairman .....	1
Opening Statement of Senator Claire McCaskill, Ranking Member .....	3

## PANEL OF WITNESSES

Linda Blase, Proprietor, Linda Blase Photography and Design, and Recipient of Spoofed Calls and Robocalls .....	5
Henning Schulzrinne, Levi Professor of Computer Science and Electrical En- gineering, Columbia University .....	6
Lois Greisman, Associate Director, Division of Marketing Practices, Bureau of Consumer Protection, U.S. Federal Trade Commission .....	8
Joe Dandurand, Deputy Attorney General, State of Missouri .....	10

## APPENDIX

### PREPARED WITNESS STATEMENTS

Linda Blase, Proprietor, Linda Blase Photography and Design, and Recipient of Spoofed Calls and Robocalls .....	29
Henning Schulzrinne, Levi Professor of Computer Science and Electrical En- gineering, Columbia University .....	32
Lois Greisman, Associate Director, Division of Marketing Practices, Bureau of Consumer Protection, U.S. Federal Trade Commission .....	39
Joe Dandurand, Deputy Attorney General, State of Missouri .....	59

### STATEMENTS FOR THE RECORD

Exhibit A: Letter from the National Association of Attorneys General, dated September 9, 2014 .....	69
Exhibit B: 2015 News Archive Regarding Phone Companies Blocking Tele- marketing Calls .....	74



# **RINGING OFF THE HOOK: EXAMINING THE PROLIFERATION OF UNWANTED CALLS**

**WEDNESDAY, JUNE 10, 2015**

U.S. SENATE,  
SPECIAL COMMITTEE ON AGING,  
*Washington, DC.*

The Committee met, pursuant to notice, at 2:32 p.m., Room 562, Dirksen Senate Office Building, Hon. Susan M. Collins, Chairman of the Committee, presiding.

Present: Senators Collins, Heller, Tillis, McCaskill, Casey, Blumenthal, Donnelly, and Kaine.

## **OPENING STATEMENT OF SENATOR SUSAN M. COLLINS, CHAIRMAN**

The CHAIRMAN. Good afternoon. When Congress passed legislation creating the National Do Not Call Registry in 2003, we thought we had put an end to the plague of unwelcome telemarketers who were interrupting Americans morning, noon, and night, but now, nearly 12 years later, phones are once again ringing off the hook. In this hearing, we will look at why Americans who have signed up for the Do Not Call Registry are still getting unwanted phone calls and what can be done to stop it.

We will see that a large part of the problem traces to the fact that the regulatory framework behind the Do Not Call List has been rendered ineffective by advances in technology. It used to be that phone calls were routed through equipment that was costly and complicated to operate. High-volume calling was difficult and expensive, especially for international calls. That old equipment could not be used easily to disguise or spoof a caller ID.

Now, phone calls can be routed from anywhere in the world at practically no cost. This can be done by using so-called Voice over Internet Protocol technology, or VoIP, and the computer programs needed to generate these calls are remarkably inexpensive and easy to use.

Now, reputable telemarketers scrub their calling list against a data base to make sure that they do not dial numbers belonging to consumers who have signed up for the Do Not Call List. If you are on that list, there is a good chance that the telemarketer who is calling you is not legitimate. Instead, it could well be a scam artist using a computer programmed to generate robocalls. These robocalls typically originate offshore, often from call centers in India, but you would not know that fact from looking at your caller

ID, because the scammers spoof their caller ID to add credibility and hide their true location.

As we learned in our recent hearing on the IRS scam, fraudsters can even spoof their numbers to make victims believe that they are calling from the IRS or local law enforcement. When these unsuspecting victims see the Internal Revenue Service or their local police department pop up on their caller ID screen, they are worried, scared, and often easily hustled into doing whatever the scammers demand.

Simply put, spoofing is very easy, as I will now demonstrate.

[Telephone ringing.]

The CHAIRMAN. My screen is reading, "Internal Revenue Service," but let us see. Hello, this is Susan Collins. May I ask who is calling?

Mr. DEWEY. Hello, Chairman Collins. This is Sam Dewey from your staff.

The CHAIRMAN. Sam, my phone says that you are calling from the IRS headquarters number, which is 202-622-5000. Are you calling from the IRS?

Mr. DEWEY. No, Senator, I am actually over here.

The CHAIRMAN. There you have it. Thank you, Sam.

Here is what the number would look like on a standard landline phone, where you have the screen where your caller ID shows up.

Now, the IRS, of course, is part of the Department of Treasury. My staff was able to spoof that number using a free iPhone app right here in this hearing room, and looking at my phone, I would have no way of knowing that it was not really the IRS or the Department of Treasury calling me.

Obviously, these fraudsters have no intention of following U.S. law. In fact, they may use the Do Not Call List as a source of working numbers in their hunt for new victims. If we are going to win the fight against scammers targeting our seniors, we need to get ahead of the technology that they use to generate robocalls and to spoof caller IDs.

[Telephone ringing.]

Let us see who this one is. Hello, this is Susan Collins.

Mr. DEWEY. Hello, Senator Collins. It is Sam Dewey from your staff again.

The CHAIRMAN. Sam, this is getting old. [Laughter.]

This time, Sam is pretending to be from the Department of Justice, and he has just demonstrated how easy it is to spoof multiple phone numbers, not just the IRS, the Department of Justice, and virtually any other official sounding number, and he has also demonstrated just how annoying these repeated calls can be to the consumer, so Sam, I am turning off my ringer now.

This is a serious problem. It would be one thing if the real number were showing up on the hard line ID screen. Then callers might have some chance of protecting themselves by simply not answering the phone, as we have advised in many of our hearings, but when you see the IRS or your local police department's number, or the FBI's number showing up on your screen, you are going to answer that call.

I wish that Senator McCaskill were here right now. She will be coming—

Senator McCASKILL. I am here.

The CHAIRMAN. You managed to miss my very exciting opening statement, which had two spoofed calls during it.

Senator McCASKILL. Oh, darn.

The CHAIRMAN. You are here for the praise part of the hearing, and I do want to salute you for the work that you have done on the Commerce Committee on this issue and for the legislation that you have drafted, which I am very pleased to join you in cosponsoring, so before we turn to our witnesses whose testimony I am very much looking forward to, I now would like to call on our Ranking Member to deliver her statement.

**OPENING STATEMENT OF SENATOR  
CLAIRE McCASKILL, RANKING MEMBER**

Senator McCASKILL. First, my most sincere apologies. You know, this place is—all my colleagues will attest to the fact that all best plans get blown up by crises of schedule, so I apologize for being a few minutes late and I apologize for missing your opening statement.

Thank you so much, Chairman Collins, for holding this hearing. This is a topic I am very concerned about and, frankly, I think anybody who—and I know the witnesses here from the Missouri Attorney General's Office can speak to this—if there is one topic that comes up frequently with Missourians when I am talking to them, it really is, “Can you not do anything about the robocalls? I am on the Do Not Call List. Why can you not get them to stop?”

I watched my mother get victimized when she thought she was being called by Medicare and it was really a company called Med Care that was robocalling her and lying to her about whether or not they had talked to her doctor.

In our 2013 subcommittee hearing in the Commerce Committee, we heard about the inability of enforcement agencies to keep up with this game of whack-a-mole that phone scams have become, and pleas for help from consumers, that their providers please help them by offering technologies that will block unwanted and fraudulent calls.

I have been tough on the phone companies, not because they are causing the problem, but rather because they are in the best position to do something about it. Some innovators have made great strides in developing call-blocking technologies. However, to my frustration, industry representatives have continued to insist that the law does not allow them to do this. That does not work.

I was not the only one seeking clarity here. Missouri's Attorney General, Chris Koster, a Democrat, along with Indiana's Republican Attorney General, spearheaded a letter to the FCC and 37 other Attorneys General signed on. They wanted a formal opinion that clarified whether what we were hearing from industry was true, that their hands were tied about their ability to provide call-blocking technology based on consumer choice.

I am pleased today that we are joined by Missouri's Deputy Attorney General, former Judge Joe Dandurand, to explain why giving consumers more power and choice in which calls they receive is such an important concern for law enforcement nationwide.

I am also pleased that FCC Commissioner Wheeler has heard concerns coming from Capitol Hill and across the country and recently announced a proposal to be considered at the Commission later this month that would allow telecommunications providers to offer consumers technology tools to combat unwanted calls. This proposal will be voted on next week at the FCC, and I am strongly encouraging the FCC to adopt Chairman Wheeler's proposal.

I am grateful that the FCC has used its existing authority to modernize its rules. However, I also recognize that in some cases, statutory changes must be made to keep up with rapidly evolving technology. To that end, this week, I have introduced and am very pleased to have cosponsorship with the chairman of this Committee, Chairman Collins. We introduced together the Robocall and Call Spoofing Enforcement Improvement Act. This bill would give the FCC more enforcement authority, allowing it to go after non-licensed robocall violators and increasing penalties on them.

One of the other concerns we have heard from our law enforcement agencies is their inability to get at spammers who spoof calls from overseas. This bill would allow for the FCC to enforce our spoofing laws against overseas callers who direct their activities to those living in the United States.

Additionally, the bill would grant the FCC explicit authority to regulate third-party spoofing services.

We have to stay on top of this issue because spammers, spoofers, and robocallers will continue to use whatever tools are available to them to defraud American consumers and America's seniors. We must give them the flexibility to fight these fraudsters. The complaints are only increasing. In the last five years alone, the FTC reports monthly complaints about illegal robocalls have doubled.

In Missouri, as we will hear from Attorney General Dandurand, the top complaint of residents is unwanted and illegal telemarketing calls. It is not even close. His office gets 50 times the number of complaints for those calls than it did for the next highest category of complaint.

We can do this. Together, we can do this. I look forward to hearing the testimony from this panel and exploring more ways to help consumers fight these unwanted calls.

Thank you, and I look forward to all of your testimony.

The CHAIRMAN. Thank you very much for your statement.

I would note that we have been joined by Senator Heller, Senator Casey, and Senator Kaine, and I know that others of our colleagues will be joining us as their schedules permit.

We now turn to our panel of witnesses. First, we will hear from Linda Blase, a lighting designer and photographer from Dallas, Texas. She will tell us about the constant barrage of unwanted telemarketing calls she has received despite registering with the Do Not Call List.

Second, we will hear from Professor Henning Schulzrinne from Columbia University in New York. The professor will explain the technology and describe the work that he is doing with the industry standards setting groups.

Third, we will hear from Ms. Lois Greisman, who is the Associate Director of the Division of Marketing Practices in the Bureau of Consumer Protection at the Federal Trade Commission.



Finally, we will hear from Joe Dandurand, who is the Deputy Attorney General in Missouri.

I want to thank all of you for joining us, and we will start with you, Ms. Blase.

**STATEMENT OF LINDA BLASE, PROPRIETOR,  
LINDA BLASE PHOTOGRAPHY AND DESIGN, AND  
RECIPIENT OF SPOOFED CALLS AND ROBOCALLS**

Ms. BLASE. Chairman Collins, Ranking Member McCaskill, and members of the Committee, thank you for giving me the opportunity to speak for thousands of American citizens who constantly receive unwanted telephone solicitations.

As a small business owner working out of my home, my phone number has also found its way to telemarketers who target business. I know there are more critical issues to address in today's world, but there are few that affect as many of us on a daily basis as the barrage of robocalls that constantly interrupt our lives.

In addition to scammers posing as the IRS and the FBI, trying to steal my savings, I have been bombarded by unwanted and irrelevant sales calls. I have had telemarketers tell me that my credit card processor is not in compliance with government regulations and their company needs to come upgrade it immediately, as if I ever had a credit card processor.

One tried to sell me an ATM. Maybe I could put it in my living room.

Several had important information about my credit card account, adding that there is no problem right now, but this is my last chance for them to lower my interest rate. If only that were true. I have been getting these calls for years, and then there is the man who starts out with, "Hello, seniors," and then tries to sell me a device that calls for help if I fall. Oh, and by the way, someone has already paid to set it up for me, about a dozen times.

These are just a few examples of the calls we are all getting every day.

When the Do Not Call List was established, I immediately registered my phone number, but it soon became clear that it made no difference to these people. All they had to do was change a number or spoof one to hide their identities and evade prosecution, and that is assuming anyone was even willing to invest the time and energy required to do so, and with the proliferation of robocalls, it got even worse. If you actually speak to a human being and ask where the company got your phone number, if they do not hang up immediately, they will tell you they have no idea. They just get on the line after the computer has dialed your number and you answer the phone, and since toll free numbers apparently are not public record, telemarketers can hide their identities that way.

I am reminded of the Borg mantra on Star Trek. Resistance is futile. There are too many ways these unethical people can invade our homes incessantly and with impunity, day in and day out.

If you answer these calls or press one to speak to a sales rep, or press two to be taken off their list, you are just making matters worse. You have effectively told a computer that it has reached a working number. It also knows that you will answer calls from numbers you do not recognize, so not only will it continue to call

you, your number may go on a list of targeted numbers which can be sold and resold many times to a multitude of telemarketers, robocallers, and scammers, so you have very few options. You can do a quick pick-up and hang-up without saying a word, or you cannot answer, giving the call a chance to go to voice mail, where you have to spend the time to retrieve and delete the number. You can report the numbers to the FCC using a detailed and time consuming online form, which I have done several times, or you can go to a consumer-driven website that collects complaints from others who are also tearing their hair out over these calls. It is all an exercise in futility.

In search of a solution to the problem, I agreed to participate in a Consumers Union campaign against unwanted robocalls. I found that while call blockers can be useful straight out of the box, their effectiveness is limited, and to be fully functional may require additional and sometimes complicated programming, and my aging brain is looking for more simplicity, not more complication.

It would be so much simpler if the phone companies could just block calls from their telemarketing clients to all numbers on the Do Not Call List, or to provide free robocall blocking tools to their residential and business customers, or both.

As far as I am concerned, these calls are unwanted intrusions into my home, and scammers prey disproportionately on our elderly citizens. Why should telemarketers be exempt from regulations similar to the common requirement for door-to-door salespersons to skip homes with a “No Solicitors” sign posted near the door? We need a similar mechanism for these unwanted phone calls. The National Do Not Call Registry was supposed to do this, but the technology used by the robocallers has made enforcement nearly impossible.

I believe the telephone companies have the ability to do more in this area and that they should do so. We are certainly paying enough for their services. It is time for us all to take a good look at this issue and work together to stop or at least sharply decrease the number of these unwanted and fraudulent calls.

Thank you for your time.

The CHAIRMAN. Thank you very much for your testimony. When we get to questions, I am going to ask you about the robocall log that you kept for a month. I think it is very illuminating, the dozens of calls that you received and the variety of them.

Professor, we look forward to hearing from you next.

**STATEMENT OF HENNING SCHULZRINNE, LEVI  
PROFESSOR OF COMPUTER SCIENCE AND ELECTRICAL  
ENGINEERING, COLUMBIA UNIVERSITY**

Mr. SCHULZRINNE. Thank you. Chairman Collins, Ranking Member McCaskill, and members of the Committee, thank you for the opportunity to appear before you today. My name is Henning Schulzrinne and I am the Levi Professor of Computer Science and Electrical Engineering at Columbia University in New York. I was the Chief Technology at the FCC from 2012 to 2014 and currently serve as a technology advisor to the FCC. I am pleased to join you to discuss technology issues and potential solutions surrounding robocalls and number spoofing. The views I express today are my own and do not necessarily reflect those of the FCC.

Illegal and more general unwanted robocalls come in many flavors. We heard a few of those described in great detail already. All are annoying. Some are harassing, threatening, or deceptive. Beyond the well-known IRS and tech support scams, similar technology also facilitates swatting, that is, false 911 calls claiming a crime in progress, or telephony denial of service attacks that interfere with the operation of nursing homes, hospitals, and other institutions.

All of these, as distinct as they may seem, leverage the same three enablers: Cheap and anonymous international phone calls, as you mentioned; easy spoofing of a telephone number, whether it looks like a real number, like the IRS, or a law enforcement agency, or even complete nonexisting numbers that are used simply to obfuscate the origin; and fake or misleading caller name information.

Fortunately, while new technologies have enabled the scourge of unwanted calls, emerging technologies can also help reduce and, I hope, eventually eliminate these calls. In my written testimony, I describe eight tools that are being developed. They are, however, reliant on three key concepts that I will outline now.

First, we need to make caller ID information trustworthy again.

Second, we need to provide traceable and reliable caller name information, and third, we need to let consumers and businesses decide which calls they want to receive and which ones they do not.

These techniques, as different as they seem, attack unwanted calls by making it harder and more expensive for fraudulent callers to reach their marks and make it easier for enforcement authorities, such as the FCC and FTC and the State Attorney Generals, to locate and shut down these operations.

Let me start on the first topic. First, to ensure that only entities authorized to use a telephone number can place calls using that number, the STIR working group within the Internet Engineering Task Force, known as IETF, is finishing up a set of specifications that allow legitimate originators of calls to cryptographically sign call set-up messages. I am helping that working group, as well.

The technology is very similar to what is currently used to sign websites that are used by, for example, banks or other financial institutions. These techniques can be implemented as Voice over IP calls reach traditional phone networks, and thus, they can protect legacy networks even though we may not be able to upgrade those technologies themselves. Thus, they are able to protect both landline and mobile subscribers from fake caller ID information.

However, I believe that even before we can implement cryptographic validation on a large scale, we can prevent the spoofing of numbers used by the kind of institutions mentioned—by banks, government offices such as the IRS, and social service agencies. I have called this approach the “Do Not Originate List,” as a rough equivalent to the Do Not Call Lists. Organizations who are likely to be impersonated by fraudsters would provide their numbers to operators of Voice over IP gateways, letting them know that no legitimate call would use those numbers. Gateway operators can then either remove or translate the bogus caller ID information. For example, all such calls with fake caller ID may then appear as area code 666.

Second, Voice over IP technology allows making caller name information more reliable, as we no longer have to rely on a very short string derived from a third-party data base which can, indeed, be substituted with a similar looking name. A new working group within the same standardization organization has been proposed to modernize the delivery of caller name information.

Third, and importantly, consumers and businesses need the technical ability to decide which calls to receive. They may either want a black list or white list. A black list designates numbers to be blocked, redirected to voice mail, or subject to a “are you human” test. These would be derived, for example, through crowdsourcing. A white list allows only certain numbers to reach, say, vulnerable individuals, while other calls are either blocked or forwarded to a family member or other trusted third parties.

Importantly, such black lists and white lists can be implemented either by telephone providers themselves, or, if those providers cooperate, by making it possible by consumers’ chosen third parties to vet phone calls, and these third parties can then compete on who does the best job of filtering out unwanted calls. This does, however, require that phone companies provide the suitable interfaces to do that.

I appreciate your interest in this topic and I look forward to your questions on the technology. Thank you.

The CHAIRMAN. Thank you very much, Professor. I very much appreciate your testimony.

Ms. Greisman.

**STATEMENT OF LOIS GREISMAN, ASSOCIATE DIRECTOR,  
DIVISION OF MARKETING PRACTICES, BUREAU OF  
CONSUMER PROTECTION, U.S. FEDERAL TRADE COMMISSION**

Ms. GREISMAN. Thank you very much. Good afternoon, Chairman Collins, Ranking Member McCaskill, and members of the Committee. I am delighted to appear before you to discuss the FTC’s work to fight illegal robocalls. I am also very pleased to be sitting next to Professor Schulzrinne, who has been a vital partner at the FTC—excuse me, at the FCC—with us.

Tackling robocalls and curbing any unwanted telemarketing, particularly calls that target seniors, is a top priority for the FTC. Eleven years ago, the Commission established the Do Not Call Registry to create an easy-to-use tool for consumers to protect their privacy against unwanted calls. I do believe that program has been highly effective in reducing calls from legitimate telemarketers.

Several years ago, as you referred to, Chairman Collins, the landscape started to shift in a very troubling way. Robocalls were on the rise. In 2009, the FTC received just a little more than 60,000 complaints about robocalls each month. Currently, we get approximately 150,000 complaints each month, a dramatic increase, so what happened?

Major technological changes in telecommunications services have led to lower costs and improved services for consumers. That is good news, but unfortunately, fraudsters also have taken advantage of these same lower costs which brought faster and cheaper automated dialing platforms. Fraudsters, as we have heard already, have also further exploited caller ID spoofing, which induces

the consumer to pick up the phone while enabling the scammer to hide anywhere in the world, hide its identity and location. In short, bad actors have taken advantage of this relatively cheap and scalable business model and used it to blast literally tens of millions of robocalls, illegal robocalls, over the course of one day at a cost of less than one cent per call.

It is bad enough that these robocalls invade consumers' privacy and are illegal. Coupled with the illegal privacy invasion, however, we all too often see that the robocallers pitch goods and services riddled with fraud.

The FTC continues to step up its law enforcement initiatives. For example, we have shut down a major robocall operation that ripped off seniors by telling them they were eligible to receive a free medical alert system bought for them by a family member or friend. Seniors who pressed one on a phone were transferred to a live operator, who said the medical alert device was approved by the American Heart Association or the American Diabetes Association. We allege those claims to be false. I think that is precisely the type of robocall that Ms. Blase referred to earlier, and I note that the State of Florida was a co-plaintiff in that case.

In another recent case filed with ten State Attorneys General, including Missouri, Indiana, North Carolina, and again, Florida, the FTC sued the telemarketer, the lead generator that provided the names, the telephone numbers, and also the companies that helped the telemarketer spoof its caller ID to hide its identity. These entities were responsible for blasting billions of robocalls attempting to sell a cruise to the Bahamas.

I do believe our coordination with State, Federal, and international partners is as strong as ever. As you know, while the FTC has no criminal enforcement authority, I am very happy to report that some of the individuals sued by the FTC for placing illegal robocalls have been prosecuted criminally by the Department of Justice.

Still, we know law enforcement is not enough. We have committed to stimulating technological solutions by issuing no less than four challenges, challenging entrepreneurs to develop solutions, such as robocall blocking services that will zap "Rachel from cardholder services" before she can invade our privacy and spew her lies. Our fourth contest takes place in August. It is entitled, "Robocalls: Humanity Strikes Back." I think that title says it all.

We think these contests have been very successful, as attested to by the fact that one of our winners of the very first contest brought his product, "Nomorobo," to the marketplace just six months after winning. Nomorobo now has 170,000 subscribers and reports to have blocked 24 million calls.

With these challenges, and as detailed in the testimony, the FTC plays a leadership role to stimulate ongoing robust dialog with technical experts, academics, and industry groups, and I do want to underscore that our work is international in scope. In fact, members of the London Action Plan and the Voice and Telephony Abuse Special Interest Group are meeting in Dublin, Ireland, as we speak to tackle the consumer protection issues robocalls present.

Finally, I want to assure you of our ongoing and sustained commitment to protect consumer privacy and halt telemarketing fraud

by enforcing the Do Not Call Registry and by tackling illegal robocalls.

I look forward to your questions. Thank you.

The CHAIRMAN. Thank you for your testimony.

Mr. Dandurand.

**STATEMENT OF JOE DANDURAND, DEPUTY  
ATTORNEY GENERAL, STATE OF MISSOURI**

Mr. DANDURAND. I take this opportunity on behalf of Attorney General Chris Koster to thank Chairman Senator Collins and my friend and Ranking Committee Member Senator Claire McCaskill and the Committee for inviting us here this afternoon, and going last, I apologize ahead of time for being a bit redundant. We have heard a lot of these things before.

The Missouri Attorney General's office has a division dedicated entirely to responding to complaints from Missouri consumers. The Consumer Protection Division receives complaints about a wide variety of scams and frauds, such as illegal debt collecting practices and identity theft. However, the number one complaint by Missourians, as Senator McCaskill indicated, by a significant margin, is about unwanted and illegal telemarketing calls.

In 2014, the vast majority of complaints our office received—of the well over 52,000 calls we received—were about illegal telemarketing. The next highest category of complaint was 1,200, just under 1,200.

As in most states Missouri's No Call allows individuals who do not want to be called by telemarketers to register both their residential and their cell phone numbers on the No Call List.

Every day, our No Call Unit receives complaints from people, many of whom are seniors, who have been abused or harassed by telemarketers who have no respect for the law or the privacy of those whom they victimize. Last month, our office received a complaint from an 80-year-old woman in St. Louis. She had received a call from someone telling her that she is eligible for a back brace paid for by Medicare. The caller was able to get the woman's Medicare identification number, which is her Social Security number and her date of birth. After hanging up the phone, she quickly realized that something was not right with that call and she notified our office.

We also frequently receive complaints about robocalls, many of which specifically target seniors. For example, one recorded message making the rounds informs the senior consumer that he or she is eligible for a free medical alert bracelet if the senior will simply provide their identifying information.

While some technologies, such as caller ID, help address unwanted calls, even then, technologies may be exploited. For example, caller ID spoofing happens when a caller deliberately falsifies the name and telephone number appearing on the caller ID information to disguise the caller's true identity, as you have seen Senator Collins be victimized here before we started today.

One of the most frequent spoofing complaints our office receives from seniors is that their caller ID relays the letters "SSI" as the caller's identity. The seniors believe, of course, the call is coming from the Social Security Administration. However, upon answering

the call, the consumer is immediately asked survey questions designed to illicit personal information.

Our office is also fighting back in the courtroom. In 2014, we obtained more than \$600,000 in judgments penalizing telemarketers for their illegal conduct, and significantly, our office also obtained court orders permanently prohibiting 28 telemarketers from ever placing another call into the State of Missouri, but they are clever and they are relentless.

Unfortunately, as Senator McCaskill told us a minute ago, it often becomes as frustrating as the old arcade game whack-a-mole. We shut them down and they pop up again in other states or with different identities. Many have resorted to setting up shop and making calls from overseas locations, effectively nullifying our ability to obtain enforcement jurisdiction over them.

This is a battle, however, which must be fought on many fronts. We need the help of private industry, including the telephone service providers, to help create solutions to help deter unwanted telemarketing calls.

Already, as you know, technologies exist to reduce the number of robocalls to consumers' phones. These, "call blockers" filter incoming telemarketing calls before they reach the consumers' phones, thus dramatically reducing the number of unwanted calls a person receives.

Yet, major phone carriers have resisted allowing the customers to have access to these call blocking technologies, claiming that Federal law prohibits it. To quote from a U.S. telecom rep at a July 10, 2013 Senate Subcommittee on Consumer Protection hearing, "The current legal framework simply does not allow phone companies to decide for the consumer which calls should be allowed to go through and which calls should be blocked."

If so, then that should be changed. If that is the only thing stopping them, then by all means, we should clarify the law and give them such power. That is why last fall, Missouri Attorney General Chris Koster and Indiana Attorney General Greg Zoeller, with whom Senator Donnelly is certainly friends, joined by the 37 other Attorneys General that Senator McCaskill referenced before, penned and submitted a letter to the FCC, which is attached to my testimony as Exhibit A.

We are thankful and encouraged by the fact that FCC Chairman Wheeler agrees. In response to the letter, Chairman Wheeler submitted a proposal to protect Americans from unwanted robocalls, spam text messages, and telemarketing calls, and it looks like the FCC will, in fact, provide clarity on the issue based on Chairman Wheeler's request. They are going to vote at the Commission's open meeting on June 18th.

Our office is encouraged by the progress we have made, but we recognize the continuing challenges that need to be addressed. Consumers have made it clear that they are fed up with the number of unwanted telemarketing calls they receive. We must continue to research and employ newer technologies to help in our efforts to keep up with the illegal robocallers. The telephone carriers are in the unique position to help their own customers block these calls. Once the major carriers are on board, we can truly make a dif-

ference in the lives of consumers by giving them the power to stop the illegal telemarketing phone calls at their inception.

While we do not share the industry's interpretation of the existing rule of law, to the extent that there is any ambiguity regarding the phone companies' legal authority to honor its customers' requests that they block these unwanted calls before they arrive, we would request clarity on that issue.

Thank you again for the opportunity to briefly testify here today.

The CHAIRMAN. Thank you very much for your testimony, as well.

Ms. Blase, as I mentioned, you kept a robocall log that you shared with the Committee. It is extraordinary how many calls that you received. You were very precise about listing all of them, and that in many cases, you would get repeat calls. You would hang up and the person would call back again.

I am curious whether you felt when you did answer some of these calls that the individuals had information about you that made the call more convincing and might be more persuasive to an individual who is less sophisticated than you are in dealing with these calls.

Ms. BLASE. Chairman Collins, the only time that I felt like they had information about me specifically was the business calls, because they got information somewhere that I have a business, so they assume I take credit cards, and they assume that I would have an ATM or would want to buy one for my business. I can only suspect that it came from the Sales and Use Tax Permit that I have to have in order to run my business or from a directory that is put out—a business directory that is put out.

In fact, I have had a lot of trouble with that business directory sending me things every year saying, if you do not return this information confirming who you are or what you do or what you sell, we are going to have to drop you from the list, so I say, hooray, drop it, but every year, I get the same one, and they describe my business as something that it is nothing like, so I suspect that they are getting my number from that business list, which, I suspect, got it from the State, but I do not know that.

The CHAIRMAN. Since not everyone has seen the call log that you put together over a month's time, could you describe in a little bit of detail the number of calls you received and the type of calls.

Ms. BLASE. Oh, gee. It is a big, long list, something like 74 calls. I put that in my written testimony, but I did not count this up, and since I sent this to you, that same caller that called five times in one day when I did not answer has called me back another couple of times.

The CHAIRMAN. This was just in a month's time.

Ms. BLASE. Yes. This is just one month's time. I started keeping this log on the 5th of May.

The CHAIRMAN. And you are, I assume, registered on the Do Not Call List.

Ms. BLASE. Oh, yes.

The CHAIRMAN. So you got more than 70 calls—

Ms. BLASE. Right.

The CHAIRMAN. [continuing]. in a month's time—

Ms. BLASE. Yes.



The CHAIRMAN. [continuing]. despite being on the list, which says something about the efficacy of the Do Not Call List.

Professor, I understand that some commercial carriers are hesitant to offer robocall filters because of a concern that they cannot legally block a call under their common carrier obligations, and as has been discussed today, the FCC Chairman has released a proposal intended to clarify this legal issue—I gather there is dispute over the legal issue—and made clear that robocall filters are legal, so in the event that the FCC accepts the Chairman’s proposal, are there robocall filters that are available now for consumers that could be put in place immediately by commercial carriers, by the telephone companies, to help protect consumers?

Mr. SCHULZRINNE. Chairman Collins, there are three types of solutions that could be deployed either immediately or within a matter of months or short of a year. One, which was already mentioned, are third-party services that essentially rely on a specific feature called simultaneous ringing that some phone systems provide, and this is where Nomorobo solution, that allow the consumer to filter calls. That solution currently is only applicable to more modern phone systems, typically provided by the cable companies, Voice over IP companies, or some of the fiber-based phone services by the traditional phone companies.

The second one which I see as particularly promising is that the phone companies would provide external interfaces, so-called APIs, Application Programming Interfaces, which would allow third parties to decide on consumers’ behalf and chosen by the consumer which calls to either block, redirect, or redirect to some third party, for example.

The third type of solution I mentioned would be apps that you could install on your phone, on your smart phone, that would block it. Currently, these apps exist, but because they have to work a little bit on the side, they are not really well integrated into the existing phone devices, they do not work all that well, so with the cooperation of carriers, these type of downloadable apps could work much better than they do today.

Just to add, the fourth one, again, is I believe that the kind of wholesale prevention of number spoofing could also make the job of enforcement much easier because it would become much more difficult for illegal telemarketers to spoof, for example, non-existing numbers, which is quite common today.

The CHAIRMAN. Thank you, and I think the point is the technology does exist for us to deal with this problem.

Senator McCaskill.

Senator McCASKILL. Thank you, Senator Collins.

Professor, is there any law that we need for the encryption to assure the validity of a caller ID? Can that be done now without any kind of change in Federal law?

Mr. SCHULZRINNE. I am not a lawyer, so—but, my sense is that adding cybersecurity—and this is an example of that—to technology does not generally require additional legal authorization, just like banks did not need to ask for the permission of the FDIC or of the Controller of the Currency to add protection to their bank websites. Indeed, longer term, I think we need to reverse the discussion, namely, what obligations do various participants have—

Senator McCASKILL. Right.

Mr. SCHULZRINNE [continuing]. to protect it—

Senator McCASKILL. Right.

Mr. SCHULZRINNE [continuing]. that information.

Senator McCASKILL. I think that—I will followup with the FCC and make sure, but I am hoping that along with the clarification, that there is no barrier to the common carriers' efforts to help consumers block this call, that they would also do what they can to encourage this encryption possibility, because I think it is a twofold problem. One is making sure the caller ID is who it says it is, and two, being able to block the calls.

Deputy Attorney General, I know your office has done great work in this area, and I know you have banned 28 telemarketers, but I am, as you know, I am an old prosecutor. Are we not going to have to start putting some people in jail? I mean, the people that are doing this, the reason it is whack-a-mole is because they do not fear any authority at this point. They are fearless of authorities. If we began picking off—and I know that is it likely that we are going to get U.S. Attorneys' Offices to get all in on this? I am painfully aware of the limitations of your office in terms of criminal prosecutions, but are there laws in Missouri that you think currently would allow you to put some of these people in prison?

Mr. DANDURAND. I do not think we have laws that give the Attorney General's Office initial—

Senator McCASKILL. What about local prosecutors? Do they have it?

Mr. DANDURAND [continuing]. jurisdiction over those.

Senator McCASKILL. Would they have local—I am trying to think what they could be—I guess they could be prosecuted under stealing by deceit.

Mr. DANDURAND. They could, and there—

Senator McCASKILL. Or attempted stealing by deceit.

Mr. DANDURAND [continuing]. the consumer protection laws are there, so if it is a criminal violation of consumer protection, if you can prove their intent, rather than a simple violation but intent to scam, which makes it more difficult, those are available, but right now, it is difficult. The feds have been helpful in that regard and there are multi-State efforts to criminally prosecute folks, so they actually are—DOJ is assisting in that regard, but we are fairly well handicapped without additional criminal jurisdiction, and as you know, that is very hard to come by, the authority.

Senator McCASKILL. Yes, and I am not even saying I am for that, but I am saying that we might want to look at what State statutes can be utilized and what communication you have with local prosecutors to help facilitate them bringing these cases. I do think the more people that are criminally prosecuted here, the more quickly you are going to clean some of this up.

Let me ask you this. Does it work when you ban these 28 telemarketers? Do they stay out? Have you caught them coming back after you have banned them?

Mr. DANDURAND. We have not caught the same named persons twice or the same named companies twice, but we certainly believe that they changed the name of the outfit and moved somewhere else, or just what they do, they network from State to State until

they get barred in another State, then continue to do this, so that whack-a-mole theory is just truly, truly difficult to get a grip on.

Senator MCCASKILL. What about cooperation from the common carriers? Ms. Greisman, you were at our hearing in 2013 and you know that—I mean, I do not get this, candidly. I think right now, if any carrier in this country came out with an ad campaign, forget about cut your bill in half, forget about “Can you hear me,” forget about look at my network and how good it is, if they came out with an ad, we are going to block robocalls, I mean, I do not think they could handle the business they would get, and I do not get why they have been dragging their feet and why it is going to take the FCC clarifying that this is not a problem.

Do you believe if the FCC votes the way we hope they are going to vote tomorrow that we will see a land rush of carriers coming to the forefront, saying, yes, we will offer this service to our customers, because Primus in Canada does it now to their customers at no charge.

Ms. GREISMAN. Well, I would like to be cautiously optimistic, but not hold my breath on it. For years now, as you know, we have informally been urging carriers to do just that, citing Primus as a perfect model. The FTC formally commented on the FCC’s proceeding, expressing its view that there is no legal impediment to providing a service that carrier subscribers are desperately asking for. We are eager to work with them, and they do participate in the various working groups that we have referred to, and again, I would like to be optimistic.

Senator MCCASKILL. Usually, American companies are so smart about marketing. I do not get why all their marketers are so dumb on this. It is just amazing to me. Thank you.

Mr. SCHULZRINNE. One reason, I believe, is that it is often sold as part of a bundle as opposed to a stand-alone service. Most people now get their voice service as part of a broadband, video, and voice bundle as opposed to—

Senator MCCASKILL. They do not think it is going to let them—I do not think they realize, we have got choices on bundles. I have got two or three places I can go for a bundle. I would much rather go for the bundle when they are going to block these robocalls, I will guarantee you that, and I bet the vast majority of Americans agree with me.

Thank you.

The CHAIRMAN. Senator Heller—no, Senator Heller has left.

Senator Tillis.

Senator TILLIS. Thank you, Madam Chair and Ranking Member. I have just gotten a copy of a bill I think you are going to be putting forward in terms of the Robocall and Call Spoofing Enforcement Improvement Act. I think there is some good thinking in there. I look forward to speaking with you about it.

I wanted to continue the line of questioning about the reason why some of the common carriers would not be motivated to do it. It would seem to me that, again, it is a product differentiation, so then, it raises the question, is there some other economic value to these calls going through? Do any of you care to speak on that?

Professor.

Mr. SCHULZRINNE. I can—the economic value differs greatly between carriers. That are usually so-called termination charges or—but my sense, not being a carrier business person, is that the amount of money they would get for termination charges is *de minimis*, particularly for the largest carriers. Most of the access charges are paid to small rural carriers, for good reasons, but they are not the ones complaining about inability to block, so large carriers get very little, particularly because they symmetrically exchange traffic with each other, so I have a hard time believing that it is simply a lost revenue one.

What I have heard informally from engineers is that, often, the voice technology that is being deployed is not seen as a revenue producing opportunity. It is essentially a must-offer technology. You have to offer voice, just like a cable company offers e-mail service, but they do not differentiate based on that, and so they seem very reluctant, in some cases, to invest resources into improving the technology they have.

Senator TILLIS. Yes, and Professor, I wanted to ask you some questions about the technology. You were talking about, I think, some of the emerging technologies for Voice over IP. It is very easy to see with the simultaneous ring, I know how that works, with the VOIP providers and how the APIs could be used and that underlying technology, or even with the cell technology.

Then, there is still this area out there with the older exchanges, non-IP based, that even if we make headway in the IP infrastructure, Voice over IP, then it seems like some of the more vulnerable areas are going to be rural, they are going to be almost disproportionately have more aged populations, the folks who still have the traditional exchanges, so what sort of technology options are there for those sorts of residences that are still in—or two generations behind, arguably, most of the telephony that younger people or people in urban areas use?

Mr. SCHULZRINNE. Senator, as the Chairman pointed out, most of these illegal or non-wanted robocalls, I would say, almost all of them originate in Voice over IP, and so they—

Senator TILLIS. They can originate there, but they could ultimately end up at a private exchange.

Mr. SCHULZRINNE. Exactly.

Senator TILLIS. That is what I was referring to.

Mr. SCHULZRINNE. What happens is there is always a gateway between those two worlds, the legacy world, if you like, the TDM world, as it is called, and the Voice over IP world, so those gateway providers are in a unique position to do exactly that filtering. They have modern, software-controlled equipment—

Senator TILLIS. At a point of entry.

Mr. SCHULZRINNE [continuing]. at the point of entry.

Senator TILLIS. What sense do you have in terms of the cost to implement—I understand what you are talking about, because it is more or less the gateway between the IP originated call and the traditional teleco exchange. What sorts of technologies exist out there today, and in rough order of magnitude, what kind of costs are we talking about?

Mr. SCHULZRINNE. Again, I am not an equipment vendor, so I do not want to speculate too much, but generally speaking, these de-

vices that are interfacing between these two walls are called session border controllers and they are designed to be highly programmable, so they already have interfaces for other purposes, such as billing, other fraud control measures that they take to prevent toll fraud, to do that, so my sense is that with existing deployed gateway technology, it requires not adding hardware but adding additional software functionality that is well within the realm of feasibility.

Senator TILLIS. Thank you very much. Thank you, Madam Chair.

The CHAIRMAN. Thank you.

Senator KAINE.

Senator KAINE. Thank you, Madam Chairwoman, and thanks to all the witnesses for being here today and your testimony.

I just noticed that earlier today it was announced that the House appropriations bill was released and it proposes for the FCC in Fiscal Year 2016 a \$315 million budget, which is a \$25 million cut below Fiscal Year 2015, and \$73 billion below the President's submitted Fiscal Year 2016 budget request. We have got a lot of budget issues, but this is an issue that demands vigorous FCC enforcement, and at the very time when we need it for this challenge and other challenges, dramatically reducing the FCC's budget seems unwise to me. That is a personal opinion.

I want to talk about the issue of sort of consumer education. I would assume that that has got to be a key part of this. There is the enforcement strategies, there is the technical approaches to solving the problem, but also on the consumer education side.

Ms. Blase, I am a little bit interested in your testimony. You know, you started to get this log because you knew that these calls were scams. What is the best way to get information out to seniors or others who might be vulnerable to scams, and what is the best advice that we should be giving them? Is it just do not do telephone solicitations? I hear my wife all the time say, "I do not do solicitation by phone," click. What is the best advice, but then what are the best channels through which to get advice to people, in your view?

Ms. BLASE. I would say the best advice is to just not answer the calls. If you answer the calls, you are giving them more information than you want them to have. If you do not answer the calls, they eventually will stop calling you, but then they will change. They will get a new number, they will try again, and they will think that maybe this time you will answer the call, so I think that is the best thing that you can do, is just not answer it.

You can get some of these robocall devices, blocking devices. You can use Nomorobo, but those things have to be programmed. You have to say, do not answer this number from this caller ID, and then when they change, which they do, then you start all over, so it is—I hate to say it again—it is whack-a-mole. It is totally whack-a-mole. There is one company that keeps calling that is associated with five different companies with a bunch of different phone numbers and you cannot chop off all those heads.

Senator KAINE. Mm-hmm.

Ms. BLASE. You know, they just go from one to the other, to the other, to the other, to the other and there is nothing you can do about it.

Senator KAINE. How about to my enforcement community experts? What is your thought about the advice we should be giving? One of the things that this Committee, I think, does very well is that we have a website. We put up information. We have a hotline for complaints. We try to use these hearings as a way to give people advice. Here is what you should do, so what is your general thought about the best advice that we should be giving to people?

Mr. DANDURAND. We have the very same information on our website and we do consumer education and awareness across the State, and another piece of advice is, it is not going to be do not answer the phone, it is this. If you answer the phone and there is any hesitation, then hang it up, because that often is what you will get. You say, "Hello," and it will be dead silence until the robocall kicks in.

The problem I see, and that is why we need the help with the blockers at its inception, is that my father will be 85 next month. He tells me, "Nobody ever calls me." I do not care for so many of those folks what we tell them or how often we tell them. If the phone rings, they are going to answer the phone and they are thrilled to talk to anybody, so we need more help than consumer education, which we beat the drum daily on, but the question is a good one.

Senator KAINE. Please, Ms. Greisman.

Ms. GREISMAN. Consumer education is a critical component of our law enforcement work and policy work. Our consumer ed message is pretty clear and it is generally consistent with what you have heard. If you pick up the phone and it is a robocaller and you do not know who it is, hang up. Do not press one, do not press two, just hang up the phone, and we disseminate that message loudly, broadly, through the AARP, through Consumer Federation of America, Consumers Union. We have tremendous outreach with our educational initiatives.

Senator KAINE. Then, Ms. Blase, back to you, so had you received consumer—you know, when you started to do the log and everything, was that just because of your own kind of innate, you were just mad at these folks, or you were suspicious, or had you—I am curious, had you received consumer education enough to know, yes, these are scams and I need to keep a record of them?

Ms. BLASE. Well, I was annoyed beyond belief and had kept just a little written thing saying, okay, this one did this, this one did that, just kept it on a piece of paper, sometimes sticky notes in my drawer, but then when Consumers Union decided to really take this on, they asked people to start keeping a log, so I changed my format from scribbling stuff down to actually making this log and did it because that is what they asked to do.

There were several places where—there were several requirements for this, where you log them, then you use a robocaller, then you turn off the robocaller and you log them again so that you can see if the robocaller—the blocker—if that made any difference, so I was mostly following their instructions on what to do, but then my attention to detail probably got out of hand and I kept a whole lot more information than I needed to.

I would like to make a correction from my further answer to your question. I went back and looked at my testimony, my written tes-

timony. The 74 calls were the number of calls that I got. Sixty-two of those calls—it was less than that before, when I sent you the log. Adding the ones that got back, 62 of those were robocalls that were not charities. Those were actual telemarketing or scam calls, so it was 62 out of 74 were horrible things.

I even kept—to answer some of the other questions—I even kept carrier locations from some of these to see if I could find some kind of a pattern, but I could not. They are all over the map.

Senator Kaine. You have an interesting story, because you kind of combined the robocalls that might be directed toward seniors with the robocalls that are directed to businesses, and you are running a business out of your house. You are not going to be that successful in your business if you just do not answer the phone, so you have got to answer the phone. Have you had conversations with other business owners about this, other small business owners, and are they experiencing the same thing, because we are kind of talking about two different kinds of scam calls and I am wondering how constant it is on the business side, especially with small businesses.

Ms. Blase. I have not talked to people, but I have gone online and looked at testimonials from business people and it is all over.

Senator Kaine. Okay.

Ms. Blase. They are all—these people call my business three times a day. I get this call five times a week. I tell them to stop calling and they keep calling, so it is pretty much rampant that it is across the board, you know.

Oh, and one more thing about people having some information. Of course, the one trying to sell the little bracelet, where it starts, “Hello, seniors,” well, he had enough information to know that I am a senior, so—

Senator Kaine. I forgot I was on a clock. I was so interested in the questions, I ran way over. Sorry, Madam Chair. Thank you all.

The Chairman. Thank you.

Senator Donnelly. You are the one who can complain to your colleague. I am going to give him a pass today, is what I am going to do.

Senator Blumenthal. I am not going to.

Senator Donnelly. Well, you are like that, Richard.

Thank you all for being here, and this is for Mr. Dandurand, the first question. In your written testimony, you cite an example of a complaint from an 80-year-old woman from St. Louis, our Ranking Member’s State, who received an unwanted call for a back brace paid for by Medicare. We have heard about these calls from seniors’ organizations, physicians, from folks in Indiana who have been on the receiving end of harassing phone calls from medical equipment suppliers offering medical equipment like back braces that they neither want nor need, and the suppliers use aggressive tactics to persuade seniors into ordering unnecessary items at Medicare’s expense. We have an obligation to protect the privacy seniors have and also to protect taxpayer dollars.

Can you talk more, or a little bit more, you know, in your position as Deputy Attorney General, about the trends you are seeing in regards to calls like these.

Mr. DANDURAND. I would, and to sort of talk about what Senator Kaine said, and Senator McCaskill, as well, funding is a big problem, and if we are going to cut funding for enforcement, we are going to have more of a problem. Our office operates on 15 percent less than we did when we started in 2009, but when we increased the ability to register your cell phones, we increased the number of phones we are responsible for from two million to four million with no more folks to deal with it, so they know that.

The trends are just, I think, somewhat, Senator Collins, away from landlines toward cell phones now that they are getting this figured out, how to get to these cell phones, and it is going to mushroom and mushroom, because so far, we still get a lot of complaints, more complaints, really, from the folks that are registered landlines, so the trends are they are getting ahead of technology and they are really working on people's cell phones, even with the sophistication those cell phones have to try to block these things.

Senator DONNELLY. Well, if you look at the Federal level here, what is the one or two things that we can do to help you?

Mr. DANDURAND. There is a No Call Working Group that the feds have right now, and all the states that want to join that do, and they stay abreast of all of the cutting edge things that are available to use, so I think that any help that we can receive, Senator McCaskill's bill that she is looking at that I have not seen yet, but hopefully is going to help with this, those sort of things will be helpful, but I have to give credit as I can to the feds for all the assistance they give to us states as it is.

Senator DONNELLY. Ms. Blase, you are a tireless bulldog on this issue, and as you look at this, you know, one of the things that has struck me is when a caller ID comes up and displays "FBI," you know, that means so many things to people in our country, and when you saw that, I am interested, how did you know that when you saw FBI that that was a scam?

Ms. BLASE. I did not know when I saw FBI. I picked up the phone and answered the call and it did not take me fifteen seconds to figure out that it was a scam, because the man said, well, we are conducting this investigation and your name popped up, and I went, why would my—and it was a drug investigation, and I said, sure, my name is going to pop up on a drug investigation, so I basically told him he was a fraud and hung up, because that is the way I felt about it. Of course, I had second thoughts and I looked up the area code and it was a Washington, D.C. area code, and I thought, oh, my goodness, what if I just really screwed up? I called my local office at the FBI and said, tell me about this. Do you have any record of any of this? They said, it is totally a scam and you did exactly the right thing.

Senator DONNELLY. If you had one or two recommendations for folks around the country as you looked—you have gone through a lot of this—what would be the one or two things that you would most say to them, here is what you really need to do when this kind of stuff starts. Number one, not pick up the phone.

Ms. BLASE. Not pick up the phone. Do not press one. Do not press two. Do not do any of those things. If you cannot pick up the phone, then that is what you should do, but too many of us have to know what is on the other end of that line. You want to know



what is there. What if it is—I have friends who are “private callers,” who want their phone numbers not to display, so you do not know when you see “private caller” if that is your friend in New Zealand or if that is somebody calling to scam you or to try to sell you something, so you are tempted to at least pick up those unknown callers or private caller things, just to find out what it is. As soon as you know what it is, hang it up. I have a friend who will not refuse to answer those. She will always pick up the phone, no matter how many times I tell her not to.

Senator DONNELLY. Thank you very much, and Madam Chair, right on time.

The CHAIRMAN. You are, indeed. You get a gold star.

Senator Blumenthal.

Senator BLUMENTHAL. Thank you, Senator Donnelly.

You know, I served as Attorney General of the State of Connecticut for 20 years. I battled against these kinds of scams, and often, we look to the FTC, because of its broader authority. We were members of a working group, and so, let me ask you first, Ms. Greisman, can you give us some examples of alleged violations that you could not pursue because of lack of authority.

Ms. GREISMAN. What I would say in that regard, where we encounter challenges, it is presented by the Common Carrier Exemption. There is a blurry line between telemarketers and carriers, and we have worked closely with our colleagues at the FCC to address this issue, where we see bad carriers, but the distinctions between carriers and non-carriers can be very gray and—

Senator BLUMENTHAL. Is that an authority problem or an enforcement—

Ms. GREISMAN. It is a jurisdictional problem. We are precluded from—the Common Carrier Exemption, I cannot recall when it dates back to, but it is part of the FTC statute.

Senator BLUMENTHAL. There is a vacuum there that has to be filled.

Ms. GREISMAN. Correct.

Senator BLUMENTHAL. Any other areas where your authority really has to be broadened to give you the enforcement jurisdiction?

Ms. GREISMAN. Nothing readily comes to mind, but let me think about that.

Senator BLUMENTHAL. I think that is the basis for legislative change, is to broaden your authority so that enforcement can be more effective, because that authority essentially turns these violations into garden variety scams. They are dressed up in new technology, but they are basically scams, con artists using a different technology, and what you need is the resources and the authority to go after them, correct?

Ms. GREISMAN. I agree. Thank you.

Senator BLUMENTHAL. You mentioned, Assistant Attorney General Dandurand, that you have been talking in the working group against some of the cutting edge issues. You used the words “cutting edge.” Can you give us some idea of what those are.

Mr. DANDURAND. Well, I would again defer to them, because I do not sit on those calls, and I do not want to talk about something I am not versed in, so our no call people who are on those calls

could do that, but I would not want to try to talk about something I am not versed in.

Senator BLUMENTHAL. What are you doing that is cutting edge, Ms. Greisman?

Ms. GREISMAN. We have traditional law enforcement, but we are also discussing on those calls with our colleagues at the State level the different types of technological solutions that we have been stimulating the marketplace to develop and also discussing our efforts to work with the common carriers, as I alluded to before, to be more proactive in their anti-fraud efforts.

Senator BLUMENTHAL. Do you have data on how often the Do Not Call Registry is abused?

Ms. GREISMAN. That is an interesting question, and I believe, Senator McCaskill, you referred to that earlier. To the best of my knowledge, we are not aware of telemarketers or others accessing the Do Not Call Registry in an improper manner. In fact, in our law enforcement work, and we have brought well over 100 cases involving the Do Not Call provisions, it is truly the exception for any single one of those telemarketers to have accessed the registry. They are getting their calling lists from lead generators, from other sources.

Senator BLUMENTHAL. Probably those other sources are readily available to them and they do not need to abuse the registry.

Ms. GREISMAN. I think that is correct.

Mr. SCHULZRINNE. I mean, just to add a technology angle to that, they can just do sequential dialing. It is easy to find out which area codes and exchanges are assigned, so they can just simply go through numbers one by one. They do not need any lists for that. On occasion, they obviously do try to target using a variety of publicly available lists, as well.

Senator BLUMENTHAL. Thank you. Well, I want to thank this panel for this very informative and helpful testimony, and thank you, Madam Chair, for having the hearing. I have 45 seconds left, which I will yield to Senator Kaine.

Senator MCCASKILL. We are never going to get over this.

Senator BLUMENTHAL. Thank you, Madam Chairman.

The CHAIRMAN. Thank you very much. I am just going to ask one final question, and then if everyone, including Senator Kaine, wants to have one final question, they are welcome to do so, also, and it is for you, Ms. Greisman.

You gave really startling statistics in your testimony. You said at the end of 2009, the FTC received approximately 63,000 complaints about illegal robocalls per month, and now that number is up to 150,000 complaints per month, so that is an explosion of complaints, and I can tell you, most people do not call the FTC and register a complaint. They do not even know that is an option, so what do you do with those 150,000 complaints that you are getting?

Ms. GREISMAN. They are incredibly valuable for law enforcement, and they are in a data base that is accessible to all of our State colleagues and our Federal colleagues. We mine the data. We generate targets from that data, so I cannot under-emphasize how critical it is for consumers to file complaints with us, and I appreciate that Ms. Blase has done just that.

The CHAIRMAN. That is very helpful to know, because I think when consumers file complaints, they often wonder, was it worth it? Was anyone listening? Did anything happen? Is anyone going to get back to me? Do you actually try to respond to the complaints?

Ms. GREISMAN. That is just not practicable——

The CHAIRMAN. Given the volume.

Ms. GREISMAN. Given the volume, it is not possible.

The CHAIRMAN. Do you have—when people put a complaint on your site, do you have a list of tips for them or advice for them to avoid becoming a victim?

Ms. GREISMAN. Absolutely. When they file a complaint online, there are lots of buttons that provide consumer education, business education, other tips on what to do.

The CHAIRMAN. I put out a seniors' newsletter that we put in Area Agencies on Aging, senior centers, et cetera, and what we are thinking of is having some sort of clip-out coupon that consumers can take with them, or that we can try using AARP to put into people's homes so they know what to do, because I think there are very few people who are like Ms. Blase and really know what is going on.

Prior to looking into this matter, if I had seen the IRS or the FBI or the Bangor, Maine Police Department come up on my landline at home, you can bet I would answer that call. Now, I hope I would have been able to discern that it was not legitimate—at least, I hope it would not be legitimate, but for most people, that is a pretty scary name or number to see come up, especially when it is the legitimate number.

Mr. DANDURAND. Madam Chair?

The CHAIRMAN. Yes.

Mr. DANDURAND. One thing we are also seeing, and I am sure you know this and it may have already been mentioned, is we are seeing e-mails now with FBI on there, as well——

The CHAIRMAN. Interesting.

Mr. DANDURAND [continuing]. telling you that you have to contact them immediately in regards to investigations that are taking place involving you and such.

The CHAIRMAN. Well, one of my hopes is that our hearing today will help to heighten public awareness, and it has been particularly valuable, Professor, to learn from you that the technology is out there, and to me, that is the most important take-away from this hearing today. I think we need to push the telephone companies, the telecoms, to implement the technology in the name of consumer protection, and I will be following the FTC's work with great interest in this area.

Senator McCaskill.

Senator MCCASKILL. While we were talking, I went on to try to file a complaint, and pretty straightforward. There is a lot of good information when you go to the home page, when you just put in "FTC robocall complaint," and then it allows you to link through to a complaint. The one thing I do not file, though, is, "Please file a complaint because it helps us catch them."

Ms. GREISMAN. That is a very good point.

Senator MCCASKILL. You know, I think that Ms. Blase made a point. You are barely, barely getting the tip of the iceberg in terms

of these complaints, and I think there are people out there like Ms. Blase who obviously is my favorite witness that we have had, like, forever, because I can tell you are just my kind of woman. It is just like, no nonsense, rack them up, let us get this thing solved, and I think there are a lot of people out there like Ms. Blase, who if they knew that filing this complaint would help you find these guys and catch them, they would be much more interested in going through the process, and so, maybe on that front page where you have all the different options of learning about how to avoid robocalls, maybe if you did a big banner, "by filing a complaint, you help us catch them," it would increase the number of complaints.

Yes, Ms. Blase.

Ms. BLASE. I think that is exactly right, because I stopped filing them. I filed several and I did not hear a word back, and nothing seemed to go away, so I did not know if it was making a difference, but if you tell me this is going to make a difference, I will go right back to doing that.

Senator MCCASKILL. There you go. You may not need anybody else to file complaints to catch the bad guys because Ms. Blase is back on it.

Thank you, Madam Chairman.

The CHAIRMAN. Senator Kaine.

Senator KAINE. I appreciate the Chairwoman allowing me to ask an additional 15 questions.

No, I do not have any other questions, Madam Chair. Thank you, and thanks to all of you.

The CHAIRMAN. Thank you.

I want to thank all of our witnesses today. This has been extremely illuminating and I think we can make a real difference here in helping the public to be more aware. I love the idea of your actually having an automatic response that goes to consumers who file complaints that tells them that it is helpful to them, and I think that would help them feel that it was worthwhile, even if it does not—if you are not responding to their specific complaint. People like to feel that they make a difference, and this panel has certainly made a difference.

This hearing is about to adjourn, if I could find my closing statement which tells me how long the record is to be open, and I have it. I want to thank all of our witnesses, and as you can see, there was a great deal of interest in this hearing today by our excellent attendance. The Committee members will have until Friday, June 19th, to submit any additional questions for the record or testimony.

I want to thank both the Majority and Minority staff for their work in putting today's hearing together.

This concludes the hearing. Thank you.

[Whereupon, at 3:53 p.m., the Committee was adjourned.]

---

---

## **APPENDIX**

---

---



---

---

## **Prepared Witness Statements**

---

---





Testimony Of Linda Blase  
Ringing Off the Hook: Examining the Proliferation of Unwanted Calls  
Special Committee On Aging  
United States Senate  
June 10, 2015

Chairman Collins, Ranking Member McCaskill and members of the committee:

Thank you for giving me the opportunity to tell a story shared by hundreds of thousands of American citizens. While I know you have many more weighty issues to consider, there are few that affect as many of us on a daily basis as the barrage of robocalls that constantly interrupt our lives.

I have been called by the FBI because my name “popped up” in a drug investigation.

I have been called by the IRS, presumably wanting me to transfer funds to pay back taxes and penalties.

I have been called by a legitimate theater company that wanted to sell me something that had nothing to do with theater tickets.

Of course none of these calls came from those organizations. All were fraudulent, with spoofed names and numbers, and two of the three were scammers trying to get into my bank account.

In the first case, the caller ID actually displayed “FBI.” So I answered. It took about 15 seconds for me to tell the caller that he was a fraud, and hang up. Then, just in case it MIGHT have been a legitimate (though clearly mistaken!) call, I checked the area code and discovered it was from the Washington, DC area. What if I had just hung up on the FBI? So I called the local (Dallas) branch of the FBI. The person I spoke to confirmed that it was a scam and told me I had done exactly the right thing when I hung up on the caller.

There was no doubt about the fraudulent nature of the IRS call - the caller ID read UNKNOWN NAME. (!) I didn’t answer the call, but it went to voice mail, and of course, the robotic computer voice started talking right through my outgoing message. So all I heard was “Department number...” and a phone number. I called it. As soon as I heard “IRS” I hung up, and probably said something not very nice before I did so.

These are just a few examples of the endless nuisance calls I have received for years. I sometimes get as many as six of these calls per day; some of them are repeated multiple times. I get far more junk calls on my home phone than legitimate calls from people I actually want to speak to. Between May 5 and June 5, I had only 6 days without one of those calls. And during that time, I received 51 nuisance calls, plus 6 more that were blocked, 5 charity calls, 11 legitimate calls, and one wrong number. So 57 out of 74 were unsolicited sales or scam calls, not counting calls from charities.

When the National Do Not Call list was established, I registered my phone number.

It soon became clear that it made no difference to these people. All they had to do was change a number, or spoof one, to hide their identities and evade prosecution (if anyone was even willing to invest the time and energy required to prosecute). And when it became really easy to just feed a list of numbers into a computer and have the computer dial them repeatedly, it got even worse.

And since TOLL FREE CALLERS (800 and 888 numbers, for example) are not public record, telemarketers can use those numbers to hide their identities.

So there are many ways these robocallers can invade our homes incessantly, and with impunity, day in and day out.

Often the recorded message will ask you to “Press 1” to speak to a customer service agent. If you press 1 to ask the “agent” to take your number off their call list, they may call you obscene names before they quickly hang up on you. And then your number may go onto a list of consumers who are willing to answer unfamiliar numbers, and that list will be sold and resold many times, so a multitude of scammers can add your number to their lists.

Sometimes they offer you the option to “Press 2” to be taken off their list. You do so. Then you find that all you have done is let the computer know it has reached a working number, which it will continue to call, over and over.

So you are left with the choice of a quick pick-up and hang-up, without ever saying a word, or not answering, giving the call a chance to go to voice mail, where you have to spend the time to clear it out. You can report the calls to the FCC through a time-consuming online form, which feels like sending information into a black hole, or you can go to a consumer-driven site that collects complaints from others who are also tearing their hair out over these calls. At least that way you can get more information about the offending number from other consumers.

If I could charge for the time and energy I spend answering or following through on these calls, I could probably move into a higher tax bracket.

So when Consumers Union and the AARP decided to bring the enormity of the problem to the attention of the FCC, and to the Congress, I jumped at the chance to participate in a volunteer call blocker test for Consumers Union.

I found that while call blockers are useful, their effectiveness is limited, and to be fully functional may require some complicated programming.

The one I tested will only block a call straight out of the box if it comes in with no telephone number attached. That means that only calls that register as ANONYMOUS, PRIVATE CALLER, OUT OF AREA, or UNKNOWN showing no phone number will be blocked without additional programming. All of the nuisance calls that come in with a minimum 7-digit number will ring through. Once a call comes in, you can mark its number to be blocked in the future. But since the robocallers can (and frequently do) change their numbers, this only works until the number changes. The only consistent number in the whole process is the home phone number. So unless we change our phone numbers on a regular basis, which is impractical to say the least, or we disconnect our home phones and use only cell phones, we are largely at the mercy of the robocallers. And we all know the plague has already begun to creep onto our mobile devices and it's only a matter of time until they are inundated as well.

The blocker I tested does allow for more complicated programming options, such as blocking entire area codes or specific numbers you choose in addition to the incoming calls you have marked to block (up to 80 numbers or area codes). But then you have to “invite” the numbers of friends who live in the blocked area codes, to prevent them from being blocked. So it can get pretty complicated (and time-

consuming) very quickly. And as I age, my brain is looking for more simplicity, not more complication.

It would be so much simpler if the phone companies could block robocalls from their telemarketing clients to all numbers on the Do Not Call List and to customers who opt-in to use free call-blocking services offered by the phone carriers.

If the government is going to trust the phone companies to collect and safeguard all that metadata for the NSA, and to retrieve the information needed to identify those deemed actionable threats to our national security (under court order of course), I would assume the phone companies also have the ability to trace the people who defy the Do Not Call List. Why don't they? And why are the telemarketers not prosecuted for their blatant disregard of that registry?

If you think I'm ticked off now, just wait until I'm lying in the hospital with a broken hip after running to the phone and tripping over the thing I absent-mindedly left in the middle of the floor, just so that Rachel from Credit Services could pressure me to transfer all my credit card balances to her "low interest" (but fee-laden) credit card account.

We are reaching the point where freedom of speech is bumping up against a citizen's right to privacy. As far as I am concerned, these calls are uninvited intrusions into my home. Why should telemarketers be exempt from regulations similar to the requirement in many communities for door-to-door salespersons to skip homes with a "NO SOLICITORS" sign posted near the door?

We need a similar mechanism for these unwanted phone calls. The National Do Not Call Registry was supposed to do this, but it has become clear that the technology used by the scammers and telemarketers has made enforcement nearly impossible. I believe the telephone companies have the ability to do more in this area and that they should do so.

It is time for us all to take a good look at this issue and work together to stop, or at least sharply limit, the occurrence of such unwanted and often fraudulent calls.

**TESTIMONY OF HENNING SCHULZRINNE**  
**Levi Professor of Computer Science and Electrical Engineering**  
**Columbia University**

**SENATE AGING COMMITTEE**

**“Ringing Off the Hook: Examining the Proliferation of Unwanted Calls”**

**June 10, 2015**

Chairman Collins, Ranking Member McCaskill, and members of the Committee, thank you for the opportunity to appear before you today. My name is Henning Schulzrinne, and I am the Levi Professor of Computer Science and Electrical Engineering at Columbia University in New York. I was the Chief Technologist at the FCC from 2012 to 2014 and currently serve as a consultant to the FCC. I am testifying in my private capacity and my views do not necessarily reflect those of the Federal Communications Commission. I am pleased to join you to discuss technological issues and potential solutions surrounding robocalls and spoofing.

## **Robocalls & Spoofing – Causes and Technical Approaches**

### **Types of Illegal Robocalls**

There are many types of robocalls, some overlapping:

- *Consumer fraud*, with the caller offering non-existing or fraudulent services or goods, such as bogus computer tech support, extended warranties, fraudulent charities or cruises. For the tech support case, the caller may install keystroke logging software to obtain personal information or install ransomware. Callers may also resell credit card data provided by the victim.
- *Extortion*, where the caller threatens the called party with deportation, arrest or prosecution if they do not wire money to settle a fictitious tax debt (e.g., “IRS scam”<sup>1</sup>).

---

<sup>1</sup> <http://www.consumer.ftc.gov/blog/scammers-continuing-pose-irs-agents>;  
<http://www.irs.gov/uac/Newsroom/IRS-Repeats-Warning-about-Phone-Scams> (“Based on the

- “Swatting”, where false 911 calls claim a crime is in progress.<sup>2</sup>
- *Telephony denial-of-service attacks* where a large volume of calls overwhelms small call centers, such as public safety answering points (911 call centers), medical facilities, nursing homes or hotels, blocking all other incoming calls.
- *CNAM fraud* where the caller collects a fraction of the dip fees from CNAM database operators when the terminating carrier queries for the caller name. (Terminating carriers typically pay a small fee, such as \$0.005, for each number lookup to the CNAM database.)
- *Premium rate fraud* where the caller leaves a message (“you have won a prize”) to entice the called party to return the call to an international number incurring high toll charges.

### Spoofing Caller ID and Caller Name Facilitates Robocalls and Other Fraud

Caller ID spoofing is used for several purposes:

- By changing the originating number, robocallers can evade filters and black lists (i.e., a set of consumer-chosen phone numbers from which the consumer does not want to receive calls), including such on-line lookup services as <http://800notes.com/>. This also facilitates telephony denial-of-service.
- Falsified caller ID information can also facilitate impersonation (e.g., when calling a bank or utility<sup>3</sup>) or to gain access to voicemail.
- Caller ID spoofing can also be used to easily obtain the caller name for a particular number, even if the caller decided to suppress the information for privacy reasons.

### The Nature of VoIP Services Facilitates Robocalling and Spoofing

The widespread availability of commercial VoIP services has facilitated both robocalls and number spoofing. VoIP services are cheap to set up and have low per-minute costs. Calls placed to the U.S. cost the same whether they originate within the United States or in another country since the originator only has to pay for local Internet access and the VoIP gateway fee. (VoIP calls travel to the country of destination via the Internet and are then handed off to gateway service providers that interconnect with the traditional phone system.)

All it takes to generate false caller ID information is a configuration of a suitable open-source or commercial call generation platform or VoIP private branch exchange (PBX), which is a private telephone network used within an enterprise. Such platforms are now widely available and can be installed in any commercial cloud-hosting service. These cloud services are often available with no more than a credit card, possibly stolen or acquired anonymously for cash at a local convenience store. Calls are typically routed through multiple VoIP call handling services before they end up at a VoIP gateway that translates them to traditional, circuit-switched calls. It is quite common that the same PBX originates calls from many different phone numbers, e.g., if it serves as a virtual PBX for a number of local branches of a chain restaurant or resells services to small businesses.

---

90,000 complaints that TIGTA has received through its telephone hotline, to date, TIGTA has identified approximately 1,100 victims who have lost an estimated \$5 million from these scams.”)

<sup>2</sup> <http://www.wzzm13.com/story/news/local/coopersville/2015/01/20/family-of-boy-convicted-in-school-swatting-it-ruined-our-life/22070055/>, <http://www.ktul.com/story/27859162/western-oklahoma-police-chief-shot-while-investigating-bomb-threat>

<sup>3</sup> This is sometimes call “vishing,” an analogy to “phishing.”

While robocalls probably differ statistically from legitimate calls, the variation among legitimate calls is sufficiently large that it is hard to filter out “bad” calls reliably. The amount of information is far more limited than the type of information available for credit card payments, where the credit card processor knows about the payment history for its customers, gets information about the nature of the transaction and knows the location of the merchant. If a telemarketer spoofs a random phone number, the downstream VoIP provider or large carrier has no way of knowing what kind of calls are typical for that number since the number is most likely not a customer. Also, by the time robocalls reach one of the larger providers, they are typically part of a large aggregate of calls, including legitimate, human-dialed consumer and business calls, legitimate automated call services and illegal robocalls. Thus, it is often difficult to reliably distinguish “good” from “bad” calls, without blocking an unacceptably large fraction of good calls. Carriers could still track complaints for specific originating numbers and refuse to do business with entities that generate an exceptionally large number of robocalls complaints relative to their call volume, but spoofing makes such tracking harder.

### **Preventing Spoofing is Helpful, but Not Sufficient, to Reduce Illegal Robocalls**

Preventing illegal robocalls from reaching consumers requires two fundamental operations: (1) identifying unwanted calls reliably; and/or (2) allowing consumers to block or redirect (“filter”) such calls. Some of the technology solutions that facilitate both identification and filtering is described below. If robocallers spoof their caller ID, they can easily bypass call filters. It is true that currently, many illegal robocalls do not spoof their caller ID (presumably so that the called party can return calls when the robocaller could only reach voicemail), but illegal telemarketers may increase spoofing as call filtering becomes more effective.

### **Spoofing CNAM**

Fraudsters may use the current CNAM (caller name) system to their advantage even if they do not spoof the phone number itself. In the current system, the carrier delivering the call to the consumer (*i.e.*, typically the local phone or cable company) queries one or more industry databases to map the caller ID information to a name. The call setup request currently only contains the number, not the name. CNAM is decentralized - many database services operate number mapping services - and some of these services appear to apply little scrutiny to the textual information that is added for a specific number. For example, these services do not always check whether the business name is a trademark of another company or corresponds to the name filed with the Secretary of State or Department of Commerce in the state the business is located. Thus, a tax debt extortion scam might associate a name like “Internal Revenue” with their number if they want to look more convincing to their victims. (In general, there does not appear to be a comprehensive list of CNAM database services; they are not registered with the FCC, for example.)

### **Technology Solutions to Reducing Robocalls**

In my opinion, there are at least eight technical solutions that, individually and in combination, can reduce robocalls:

1. Filters based on simultaneous ringing
2. Smartphone apps
3. Number signing and validation
4. Improved caller name validation



5. Consumer filters
6. Carrier filters
7. Do Not Originate
8. Honey Pots

I will describe each in turn, summarizing their operations, effectiveness, privacy, applicability, and trade-offs.

#### Filters Based on Simultaneous Ringing

**Operation:** A consumer configures their phone service to simultaneously ring all of their calls to a third-party service provider, such as Nomorobo.<sup>4</sup> The service provider sees the incoming call; if the number is in the user's white list, the service provider takes no further action and the subscriber picks up the call. If the call is on a black list, it picks up the call and then hangs up. For unknown callers, the service may challenge the caller to enter some numeric code as a CAPTCHA, forcing the caller to prove that it is human rather than a robot.

**Effectiveness:** Like many of the other filtering approaches discussed below, this approach relies on crowd sourcing (*i.e.*, users indicating whether a call was unwanted or not). Thus, this type of system becomes less effective as more robocallers spoof their caller ID.

**Privacy:** By its nature, the third party has access to every inbound call reaching the user.

**Applicability:** The system requires the cooperation of the carrier and only works for certain types of modern VoIP-based landline systems landlines,<sup>5</sup> such as those provided by cable companies, but not cellular services. Older landline systems may not support simultaneous ringing or carriers may choose not to enable the feature.

**Trade-offs:** This approach has the advantage that it works today, without modifying existing systems. However, since caller ID information is provided after the first ring, all robocalls still ring once at the subscriber. Spoofed calls may fool the system.

#### Smartphone Apps

**Operation:** A user installs an app on their smartphone. The app<sup>6</sup> monitors incoming calls and terminates blacklisted calls, redirects a call to voicemail or flags a call as a likely robocall.

**Effectiveness:** The effectiveness is similar to other filtering approaches. Since users have a choice between multiple apps, apps can compete on their effectiveness, including preventing the blocking of wanted calls. They may offer different degrees of filtering (*e.g.*, to allow a user to avoid all charity calls). Reviews on the Google Play Store for apps of this type are mixed and they do not appear to work in all cases. Apps typically require payment for access to the blacklist.

**Privacy:** Apps may differ in what information they convey to the app vendor. If the app queries the backend service for each call, that service now has a complete incoming call log. There are approaches ("Bloom filters") where the app itself would store some number of blacklisted numbers and thus avoid querying the service.

<sup>4</sup> See <https://www.nomorobo.com/>.

<sup>5</sup> For example, Nomorobo stated that its system is operational with AT&T UVerse, Comcast Xfinity voice, Optimum, Time Warner Cable, Verizon Digital Voice or Vonage, but not for many traditional TDM landline services. See <https://www.nomorobo.com/signup>.

<sup>6</sup> Examples: PrivacyStar, TrueCaller.

**Applicability:** Due to choices made by the designers of smartphone operating systems, apps only work for Android, not Apple iOS.

**Trade-offs:** Apps are available today but only for Android.

#### Number Signing and Validation

**Operation:** The originating service provider cryptographically signs the call signaling request, indicating that the caller is authorized to use the caller ID contained in the call setup message. Any carrier along the way can validate the signature and detect spoofed caller ID. A carrier may then either block the call or rewrite the caller ID to indicate that the original one was spoofed. For example, it may replace the caller ID with a number drawn from the “666” area code, allowing the called party to filter the call if desired. The Internet Engineering Task Force (IETF)<sup>7</sup> STIR working group<sup>8</sup> is working on standardizing the components needed: signaling message formats and how cryptographic keys (“certificates”) are distributed to originating carriers. The certificates would likely be assigned by one of the administrative entities managing the U.S. numbering plan, such as the Number Portability Administrator (NPAC).

**Effectiveness:** The mechanism prevents spoofing and facilitates locating illegal robocallers, but does not by itself reduce robocalls. Number signing is most effective if all or almost all originating carriers sign and most terminating carriers validate.

**Privacy:** The mechanism does not reduce caller or called party privacy. The caller can still place anonymous calls (*i.e.*, calls that suppress caller ID information at the subscriber).

**Applicability:** Number signing is only applicable to VoIP systems, not legacy systems. However, almost all robocalls originate on VoIP systems, and gateway providers that bridge between VoIP and legacy systems can perform validation.

**Trade-offs:** Call handling software at both the originating and terminating carrier needs to be modified. A system for handing out certificates to carriers needs to be established.

#### Improved Caller Name Validation

**Operation:** Instead of looking up caller ID information in a CNAM database and mapping numbers to caller names, the call signaling information in VoIP can carry caller name information “in-band” and possibly additional identifying information, such as whether the caller is a registered charity or financial institution.

**Effectiveness:** This approach does not reduce telemarketing robocalls by itself, but rather makes it more difficult for robocallers to impersonate financial institutions, charities, and government agencies. It also eliminates the current CNAM dip fee scams.

The effectiveness depends on whether the originating carrier validates the caller name information provided by their customers. Just like “green” certificates for sensitive web sites, it may be sufficient if security-sensitive callers validate their caller name information so that called parties can know whether an entity claiming to be a government agency indeed is one. For consumers and small businesses, standard identity validation techniques may be sufficient to ensure that consumers provide their actual name. These identity

<sup>7</sup> “The Internet Engineering Task Force (IETF) is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet.” See <http://www.ietf.org/about>.

<sup>8</sup> Secure Telephony Identity Revised (<https://datatracker.ietf.org/wg/stir/charter/>)



validation techniques are sometimes called dynamic knowledge-based authentication (KBA) or “out-of-wallet questions”<sup>9</sup>.

**Privacy:** This requires no additional disclosure of information from the caller to the called party. It is also likely to increase consumer privacy since the current system allows any party to map telephone numbers to names using CNAM lookup services, even for unlisted numbers.

**Applicability:** The in-band mechanism is only applicable to VoIP calls, but improved validation applies to both the existing CNAM databases and VoIP delivery.

**Trade-offs:** Transitioning to this mechanism may require additional standardization efforts, the cooperation of a large number of carriers and changes in the validation of customer information. Current CNAM displays are often limited to 15 characters, making it difficult to render more detailed information.

#### Third-Party API-based Filters

**Operation:** Third-party API filters are a variation of the earlier filtering mechanisms. Here, the carrier serving a subscriber queries a third-party service chosen by the subscriber among competing offerings, using a standardized protocol. The third party service then recommends that the call is blocked, redirected to another party, forwarded to voicemail, or completed normally, possibly with additional information that could be included in the caller ID display. In addition, the mechanism may allow subscribers to label the most recent call as unwanted (*e.g.*, using a vertical service code or “star-code”), similar to the \*57 malicious caller identification code that most phone service providers offer.

**Effectiveness:** The effectiveness is similar to other filtering solutions discussed earlier.

**Privacy:** In general, the privacy implications are similar to other filtering solutions. However, as long as subscribers do not need personal white or black lists, the carrier could query the service without revealing the destination of the call so that the third party offering the filtering service does not get to keep a call log.

**Applicability:** This mechanism works for all types of systems, including VoIP, legacy circuit-switched and cellular, although it is probably easier to implement for VoIP and cellular systems.

**Trade-offs:** Third-party filters require the least amount of consumer effort since they do not need to install any apps. Since they work for legacy systems, they could be available to all consumers.

#### Do Not Originate (DNO)

**Operation:** Gateway vendors check incoming calls against a Do-Not-Originate (DNO) list of numbers where the holder of the number has declared that such calls do not use VoIP gateways or do not use that specific provider. The DNO list may also include telephone numbers that have not yet been assigned by numbering authorities to telecommunication carriers, as such unassigned numbers are commonly used by telemarketers that spoof caller ID.<sup>10</sup>

<sup>9</sup> See [http://en.wikipedia.org/wiki/Knowledge-based\\_authentication](http://en.wikipedia.org/wiki/Knowledge-based_authentication).

<sup>10</sup> For example, it is currently possible to spoof numbers from area codes that are not in use and will most likely never be assigned, such as 311 and 911.

**Effectiveness:** This mechanism prevents only the impersonation of institutions that avail themselves of the mechanism. Organizations that would be the targets of spoofing, such as financial institutions, insurance companies and government agencies, would likely register in a DNO list. Thus, since it requires active participation by spoofing targets, the mechanism is likely to reduce, but not prevent all illegal robocalls.

**Privacy:** There are no consumer privacy implications, and the list of numbers does not need to be confidential since the entities on the list are likely to include well-known “800” and other numbers.

**Applicability:** This is only applicable to VoIP gateway providers who cooperate.

**Trade-offs:** This mechanism does not require changes in protocols, but does require a mechanism for entities wanting to add themselves to the DNOL to do so without having to contact every VoIP gateway service provider.

#### (Telephony) Honey pots

**Operation:** M<sup>3</sup>AAWG defines a telephony honeypot as follows: “A telephony honeypot is a telephone service endpoint to which calls can be directed. It may appear to callers to be a normal telephone number (*e.g.*, a typical 10-digit residential or business phone number) but is specifically designed and deployed to collect information on unwanted calls. It might automatically process calls or employ humans, is computer monitored and might be recorded.”<sup>11</sup>

**Effectiveness:** Honey pots can be used for enforcement purposes and to populate filter black lists.

**Privacy:** There appear to be no consumer privacy implications.

**Applicability:** Honey pots can be used for all kinds of telephone numbers, including mobile.

**Trade-offs:** Honey pots themselves do not prevent robocalls but can be an important part of making other mechanisms more effective.

#### Summary

A set of technical approaches, deployed incrementally, can help to make illegal robocalling unprofitable by reducing the number of households scammers can reach. Validated caller ID, a better caller name system, and user-chosen call handling can return control over their phone to consumers. Some of the systems proposed require standardization and development work, but all can be integrated into commercially-deployed VoIP systems, both landline and mobile.

---

<sup>11</sup> [https://www.maawg.org/sites/maawg/files/news/M3AAWG\\_Telephony\\_Honey Pots\\_BP-2014-08.pdf](https://www.maawg.org/sites/maawg/files/news/M3AAWG_Telephony_Honey Pots_BP-2014-08.pdf); M<sup>3</sup>AAWG is the Messaging, Malware and Mobile Anti-Abuse Working Group.

**Prepared Statement of  
The Federal Trade Commission**

**Before the  
United States Senate  
Special Committee on Aging**

**on**

**Combatting Illegal Robocalls: Initiatives to End the Epidemic**

**Washington, DC  
June 10, 2015**

Chairman Collins, Ranking Member McCaskill, and members of the Committee, I am Lois Greisman, Associate Director of the Division of Marketing Practices, Bureau of Consumer Protection at the Federal Trade Commission (“Commission” or “FTC”).<sup>1</sup> I appreciate the opportunity to appear before you today to discuss the Commission’s initiatives to fight illegal robocalls, including those that target seniors.<sup>2</sup>

In 2003, the FTC responded to enormous public frustration with unsolicited sales calls and amended the Telemarketing Sales Rule (“TSR”) to create a national Do Not Call Registry.<sup>3</sup> The Registry, which includes more than 217 million active telephone numbers,<sup>4</sup> has been tremendously successful in protecting consumers’ privacy from the unwanted calls of tens of thousands of legitimate telemarketers who subscribe to the Registry each year.<sup>5</sup> More recently,

---

<sup>1</sup> The views expressed in this statement represent the views of the Commission. My oral presentation and responses to questions are my own and do not necessarily reflect the views of the Commission or any individual Commissioner.

<sup>2</sup> See, e.g., *FTC v. Worldwide Info. Servs., Inc.*, No. 14-cv-8-ORL-28DAB (M.D. Fla. Jan. 13, 2014), available at <https://www.ftc.gov/enforcement/cases-proceedings/132-3175/worldwide-info-services-inc>; see generally *FTC v. Inbound Call Experts, LLC, et al.*, No. 14-cv-81395-KAM (S.D. Fla. Nov. 10, 2014), available at <https://www.ftc.gov/enforcement/cases-proceedings/132-3135/inbound-call-experts-llc>; *FTC v. Consumer Collection Advocates, Corp., et al.*, No. 14-cv-62491-BB (S.D. Fla. Nov. 3, 2014), available at <https://www.ftc.gov/enforcement/cases-proceedings/142-3082/consumer-collection-advocates-corp>; *FTC v. Instant Response Sys. LLC, et al.*, No. 113-cv-0976 (E.D.N.Y. Mar. 11, 2013), available at <https://www.ftc.gov/enforcement/cases-proceedings/1223041/instant-response-systems-llc-et-al>.

<sup>3</sup> 68 Fed. Reg. 4580 (Jan. 29, 2003); 16 C.F.R. Part 310. The FTC issued the TSR pursuant to the Telemarketing and Consumer Fraud and Abuse Prevention Act, 15 U.S.C. §§ 6101-6108. See generally The Telemarketing Sales Rule, 16 C.F.R. Part 310.

<sup>4</sup> See National Do Not Call Registry Active Registrations and Complaint Figures. National Do Not Call Registry Data Book FY 2014 at 4 (Nov. 2014), available at <https://www.ftc.gov/reports/national-do-not-call-registry-data-book-fiscal-year-2014>.

<sup>5</sup> For example, in fiscal year 2014, more than 26,000 telemarketers accessed the Do Not Call Registry. National Do Not Call Registry Data Book FY 2012 at 8 (Nov. 2014), available at <https://www.ftc.gov/reports/national-do-not-call-registry-data-book-fiscal-year-2014>.

changes in technology led to a new source of immense frustration – the blasting of prerecorded messages that primarily rely on Voice over Internet Protocol (“VoIP”) technology.<sup>6</sup> In 2008, the Commission responded by amending the TSR to prohibit the vast majority of prerecorded sales calls.<sup>7</sup>

Illegal robocalls remain a significant consumer protection problem because they repeatedly disturb consumers’ privacy and frequently peddle fraudulent goods and services that cause significant economic harm. The FTC is using every tool at its disposal to fight them.<sup>8</sup> This testimony describes the Commission’s efforts to stop telemarketer violations, including our aggressive law enforcement, initiatives to spur technological solutions, and robust consumer and business outreach.

#### **I. Law Enforcement**

Since establishing the Do Not Call Registry in 2003,<sup>9</sup> the Commission has fought vigorously to protect consumers’ privacy from unwanted calls. Indeed, since the Commission began enforcing the Do Not Call provisions of the TSR in 2004, the Commission has brought

---

<sup>6</sup> See Section II(A), *infra*.

<sup>7</sup> 73 Fed. Reg. 51164 (Aug. 29, 2008); 16 C.F.R. Part 310.4(b)(1)(v).

<sup>8</sup> See FTC Robocall Initiatives, <http://www.ftc.gov/robocalls> (last visited June 2, 2015).

<sup>9</sup> In 2003, two different district courts issued rulings enjoining the Do Not Call Registry. See Press Release, FTC Files Motion to Stay Pending Appeal in Oklahoma DNC Ruling (Mar. 24, 2003), available at <https://www.ftc.gov/news-events/press-releases/2003/09/ftc-files-motion-stay-pending-appeal-oklahoma-dnc-ruling>; Press Release, Statement of FTC Chairman Timothy J. Muris (Sept. 26, 2003), available at <https://www.ftc.gov/news-events/press-releases/2003/09/statement-ftc-chairman-timothy-j-muris>. Congress addressed the first decision in summary fashion by enacting HR 3161 in one day. See “HR 3161 (108<sup>th</sup>) Do-Not-Call-Registry bill,” <http://www.govtrack.us/congress/bills/108/hr3161>. Press Release, Statement of FTC Chairman Timothy J. Muris (Sept. 25, 2003), available at <https://www.ftc.gov/news-events/press-releases/2003/09/statement-ftc-chairman-timothy-j-muris-0>. The 10<sup>th</sup> Circuit reversed the second district court decision on February 17, 2004. See Press Release, Appeals Court Upholds Constitutionality of National Do Not Call Registry (Feb. 17, 2004), available at <https://www.ftc.gov/news-events/press-releases/2004/02/appeals-court-upholds-constitutionality-national-do-not-call>.



120 enforcement actions seeking civil penalties,<sup>10</sup> restitution for victims of telemarketing scams, and disgorgement of ill-gotten gains against 377 corporations and 298 individuals. From the 110 cases that have been resolved thus far, the courts have awarded judgments of over \$1 billion in equitable monetary relief and civil penalties, of which the Commission has collected over \$100 million.<sup>11</sup>

#### **A. Robocall Law Enforcement**

On September 1, 2009, new TSR provisions went into effect prohibiting the vast majority of robocalls selling a good or service.<sup>12</sup> The robocall provisions cover prerecorded calls to all consumers, including those who have not registered their phone number on the Do Not Call Registry. The Commission has been aggressive in enforcing prohibitions against robocalls, filing 37 cases against 121 companies and 90 individuals responsible for *billions of illegal robocalls*.<sup>13</sup> The 34 cases that have concluded thus far have resulted in judgments totaling more than \$485 million in civil penalties, redress, or disgorgement.<sup>14</sup>

---

<sup>10</sup> As is true of all TSR violations, telemarketers who violate the Do Not Call provisions are subject to civil penalties of up to \$16,000 per violation. 15 U.S.C. § 45(m)(1)(A); 16 C.F.R. 1.98(d).

<sup>11</sup> We appreciate the significant difference between the amounts ordered and collected. Fraudsters tend to rapidly dissipate ill-gotten gains. We strive to locate as much money as practicable in each case.

<sup>12</sup> Like the other provisions of the TSR, the robocall provisions do not apply to non-sales calls, such as calls placed by charities or those that are purely political, informational, or survey calls. See generally “Complying with the Telemarketing Sales Rule” (Feb. 2011), *available at* <https://www.ftc.gov/tips-advice/business-center/guidance/complying-telemarketing-sales-rule>. Limited exceptions exist for calls that deliver a healthcare message made by an entity covered by the Health Insurance Portability and Accountability Act, 16 C.F.R. Part 310.4(b)(1)(v)(D), and for certain calls placed by telemarketers who solicit charitable contributions, 16 C.F.R. Part 310.4(b)(1)(v)(B).

<sup>13</sup> The FTC filed 12 of the 37 cases before the rule change went into effect on September 1, 2009.

<sup>14</sup> The agency has collected \$28 million of the total judgments awarded. Some of the Commission’s early robocall cases were against companies with household names such as Talbots, Dish Network, and DIRECTV. See *U.S. v. The Talbots, Inc.*, No. 10-cv-10698 (D. Mass. Apr. 27, 2010),

Yet increasingly, fraudsters, who often hide in other countries in an attempt to escape detection and punishment, make robocalls that harass and defraud consumers. For example, in *FTC v. Navestad*, the Commission successfully traced and sued robocallers even after they attempted to hide their identities through fake caller IDs, shifting foreign operations, and name changes. The court found that the defendants made in excess of eight million illegal robocalls and ordered them to pay \$30 million in civil penalties and give up more than \$1.1 million in ill-gotten gains.<sup>15</sup>

Accordingly, the Commission has sought to maximize the impact of its law enforcement efforts, and targeted those that facilitated the illegal conduct to strike a blow against many law-breakers. For example, the Commission has pursued actions against “autodialers” or companies that provide the equipment or software necessary to send out millions of calls.<sup>16</sup> The Commission has also filed suit against payment processors for assisting and facilitating robocallers by providing access to the financial networks.<sup>17</sup>

---

available at <https://www.ftc.gov/news-events/press-releases/2010/04/womens-clothing-retailer-talbots-its-telemarketer-pay-total>; *U.S. v. Dish Network, LLC*, No. 3:09-cv-03073 (C.D. Ill. Feb. 4, 2010), available at <https://www.ftc.gov/news-events/press-releases/2009/03/ftc-charges-dish-network-formerly-known-echostar-multiple-do-not>; *U.S. v. DIRECTV, Inc.*, No. 09-02605 (C.D. Cal. Apr. 23, 2009), available at <https://www.ftc.gov/news-events/press-releases/2009/04/directv-comcast-pay-total-321-million-entity-specific-do-not-call>. Although the Dish case remains in litigation, the Court granted partial summary judgment against Dish in January 2015. Press Release, Court Grants Partial Summary Judgment in FTC Case Against Dish Network, Finding Company Liable for Tens of Millions of Telemarketing Violations (Jan. 21, 2015), available at <https://www.ftc.gov/news-events/press-releases/2015/01/court-grants-partial-summary-judgment-ftc-case-against-dish>.

<sup>15</sup> *FTC v. Navestad*, No. 09-CV-6329 (W.D.N.Y. Mar. 23, 2012), available at <https://www.ftc.gov/news-events/press-releases/2012/04/ftc-case-against-deceptive-robocallers-leads-record-30-million>.

<sup>16</sup> See, e.g., *FTC v. Asia Pac. Telecom, Inc.*, No. 1:10-3168 (N.D. Ill. Mar. 28, 2012), available at <https://www.ftc.gov/news-events/press-releases/2012/03/ftc-action-puts-robocallers-out-telemarketing-business>.

<sup>17</sup> In *FTC v. WV Universal Mgmt., LLC*, a Court held both the robocaller and its payment processor jointly liable for \$1.7 million for peddling bogus credit card interest rate reduction services.

## **B. Coordination with Civil Law Enforcement Partners**

As the law enforcement challenges associated with illegal telemarketing have increased, the FTC's relationships with other agencies have become increasingly important. The Commission has robust, collaborative relationships with state law enforcers, including through the National Association of Attorneys General Do Not Call working group. In addition, the FTC regularly works with the Federal Communications Commission ("FCC"), the Department of Justice, the U.S. Postal Inspection Service, and U.S. Attorneys' Offices across the country. The Commission also coordinates with its counterparts in other countries on particular cases and broader strategic matters such as caller ID "spoofing" – the practice of faking a call's identifying information. The FTC's collaboration with its partners takes many forms, including sharing information and targets, assisting with investigations, and working collaboratively on long-term policy initiatives.

The Commission also coordinates with various partners to bring law enforcement actions. For example, in March 2015, the FTC joined forces with ten state Attorneys General to file suit against Caribbean Cruise Lines and seven other companies for blasting billions of robocalls that attempted to sell consumers a cruise to the Bahamas.<sup>18</sup> In this ongoing suit, the FTC sued the telemarketer, the companies that placed the robocalls, and the companies that helped the telemarketer spoof its caller ID to hide its identity.

---

*See* Press Release, Court Finds Defendants in FTC's Treasure Your Success "Rachel Robocalls" Case Liable for \$1.7 Million (May 20, 2015), *available at* <https://www.ftc.gov/news-events/press-releases/2015/05/court-finds-defendants-ftcs-treasure-your-success-rachel>; *see also* *FTC v. Innovative Wealth Builders, Inc.*, No. 13-cv-00123 (M.D. Fla. June 5, 2013), *available at* <https://www.ftc.gov/enforcement/cases-proceedings/122-3127/innovative-wealth-builders-inc-et-al>.

<sup>18</sup> Press Release, FTC and Ten State Attorneys General Take Action Against Political Survey Robocallers Pitching Cruise Line Vacations to the Bahamas (March 4, 2015), *available at* <https://www.ftc.gov/news-events/press-releases/2015/03/ftc-ten-state-attorneys-general-take-action-against-political>. The state co-plaintiffs are Colorado, Florida, Indiana, Kansas, Mississippi, Missouri, North Carolina, Ohio, Tennessee, and Washington.



The FTC also leads robocall law enforcement “sweeps” – coordinated, simultaneous law enforcement actions – in conjunction with state and federal partners.<sup>19</sup> In 2012, the FTC and its partners mounted a concerted attack on illegal robocalls purporting to be from “Cardholder Services,” which falsely claimed they could reduce consumers’ credit card interest rates in exchange for an up-front fee, often hundreds of dollars. The FTC brought five cases against companies that were allegedly responsible for millions of these illegal calls. The Commission simultaneously announced that state law enforcement partners in Arizona, Arkansas, and Florida had filed separate law enforcement actions as part of the sweep.<sup>20</sup>

### C. Referrals for Criminal Prosecution

Although the Commission does not have criminal law enforcement authority, it recognizes the importance of criminal prosecution in deterrence. Accordingly, the Commission routinely works with federal and state criminal law enforcers through its Criminal Liaison Unit (“CLU”). Since CLU’s launch in 2003, hundreds of fraudulent telemarketers have found

<sup>19</sup> The following describe some of the telemarketing and robocall sweeps that the FTC and its law enforcement partners have conducted over the past several years: Press Release, FTC Leads Joint Law Enforcement Effort Against Companies that Allegedly Made Deceptive “Cardholder Services” Robocalls (Nov. 1, 2012), available at <https://www.ftc.gov/news-events/press-releases/2012/11/ftc-leads-joint-law-enforcement-effort-against-companies>; Press Release, FTC Settlements Put Debt Relief Operations Out of Business (May 26, 2011), available at <https://www.ftc.gov/news-events/press-releases/2011/05/ftc-settlements-put-debt-relief-operations-out-business>; Press Release, FTC Sues to Stop Robocalls with Deceptive Credit Card Interest-Rate Reduction Claims (Dec. 8, 2009), available at <https://www.ftc.gov/news-events/press-releases/2009/12/ftc-sues-stop-robocalls-deceptive-credit-card-interest-rate>; Press Release, FTC Cracks Down on Scammers Trying to Take Advantage of the Economic Downturn (July 1, 2009), available at <https://www.ftc.gov/news-events/press-releases/2009/07/ftc-cracks-down-scammers-trying-take-advantage-economic-downturn>; Press Release, FTC Announces “Operation Tele-PHONEY,” Agency’s Largest Telemarketing Sweep (May 20, 2008), available at <https://www.ftc.gov/news-events/press-releases/2008/05/ftc-announces-operation-tele-phoney-agencys-largest-telemarketing>.

<sup>20</sup> See Press Release, FTC Leads Joint Law Enforcement Effort Against Companies that Allegedly Made Deceptive “Cardholder Services” Robocalls (Nov. 1, 2012), available at <https://www.ftc.gov/news-events/press-releases/2012/11/ftc-leads-joint-law-enforcement-effort-against-companies>.

themselves facing criminal charges and prison time. In the *Voice Touch* case, for example, robocallers pitched an auto warranty scam. The FTC case shut down the scam and the Commission was able to provide almost \$3.2 million in redress to consumers as a result of the litigation.<sup>21</sup> The Office of the U.S. Attorney for the Southern District of Illinois subsequently brought criminal charges; three of the fraud's principals have pleaded guilty and gone to prison, with the two leaders of the scheme sentenced to five years in prison.<sup>22</sup>

In *Economic Relief Technologies*, Kara Singleton Adams, the leader of a scam that used robocalls to sell worthless credit card interest rate reduction services, faced criminal prosecution from the Department of Justice after the Commission shut down her operation.<sup>23</sup> A federal jury in Atlanta convicted Adams on charges of wire fraud and conspiracy and the court sentenced her to more than 17 years of imprisonment in 2012. Three of her associates in the scheme also went to prison.<sup>24</sup>

## II. Policy and Market Stimulation Initiatives

Despite the 2008 prohibition of unauthorized robocalls and the Commission's vigorous

---

<sup>21</sup> Press Release, FTC Returns Almost \$3.2 Million to Auto Warranty Robocall Victims (Aug. 31, 2011), available at <https://www.ftc.gov/news-events/press-releases/2011/08/ftc-returns-almost-32-million-auto-warranty-robocall-victims>; *FTC v. Voice Touch, Inc.*, No. 09CV2929 (N.D. Ill. Aug. 23, 2010), available at <https://www.ftc.gov/news-events/press-releases/2010/08/auto-warranty-robocaller-pay-23-million-sell-mercedes-consumer>.

<sup>22</sup> Department of Justice ("DOJ") Press Release, "Auto Warranty" Telemarketer Pleads Guilty (June 15, 2012), available at <http://www.justice.gov/sites/default/files/usao-sd-il/legacy/2014/12/10/Auto%20Warranty%20Telemarketer%20Pleads%20Guilty.pdf>; DOJ Press Release, Update on Transcontinental Warranty Case (Oct. 31, 2011), available at <http://www.justice.gov/usao/ils/Programs/VWA/transcontinental.html>.

<sup>23</sup> *FTC v. Econ. Relief Techs., LLC*, No. 09-CV-3347 (N.D. Ga. July 22, 2010), available at <https://www.ftc.gov/news-events/press-releases/2012/09/ftc-sends-refunds-victims-robocall-credit-card-interest-rate>.

<sup>24</sup> DOJ Press Release, Adams Sentenced to Over 17 Years in Prison for Multi-Million Dollar Telemarketing Fraud Scheme (Feb. 9, 2012), available at <http://www.justice.gov/archive/usao/gan/press/2012/02-09-12.html>.

enforcement efforts, technological advances have permitted law-breakers to make more robocalls for less money with a greater ability to hide their identity. For example, at the end of 2009, the FTC received approximately 63,000 complaints about illegal robocalls each month.<sup>25</sup> That number has now more than doubled - the FTC currently receives approximately 150,000 robocall complaints per month.<sup>26</sup>

#### A. Understanding the Landscape of the Robocall Problem

Recognizing that law enforcement, while critical, is not enough to solve the problem, FTC staff has aggressively sought new strategies in ongoing discussions with academic experts, telecommunications carriers, industry coordinating bodies, technology and security companies, consumers, and counterparts at federal, state, and foreign government agencies. These efforts were ramped up on October 18, 2012, when the Commission hosted a public summit on robocalls to explore these issues (the “Robocall Summit”).<sup>27</sup> Since then, as discussed below, the Commission has spurred the creation of specific groups of experts and industry members to work together and with international law enforcers to tackle this vexing consumer protection issue.

Speakers at the Robocall Summit made clear that convergence between the legacy telephone system and the Internet has allowed robocallers to engage, at very little cost, in massive, unlawful robocall campaigns that cross international borders and hide behind spoofed

<sup>25</sup> National Do Not Call Registry Data Book FY 2010 at 5 (Nov. 2010), *available at* <https://www.ftc.gov/reports/national-do-not-call-registry-data-book-fiscal-year-2010>. Since that time, the FTC began separately tracking Do Not Call complaints and robocall complaints based on information provided by the consumer.

<sup>26</sup> National Do Not Call Registry Data Book FY 2014 at 5 (Nov. 2014), *available at* <https://www.ftc.gov/reports/national-do-not-call-registry-data-book-fiscal-year-2014>.

<sup>27</sup> See generally FTC Workshop, *Robocalls: All the Rage* (Oct. 18, 2012), *available at* <https://www.ftc.gov/news-events/events-calendar/2012/10/robocalls-all-rage-ftc-summit>. A transcript of the workshop (hereinafter “Tr.”) is available at [https://www.ftc.gov/sites/default/files/documents/public\\_events/robocalls-all-rage-ftc-summit/robocallsummittranscript.pdf](https://www.ftc.gov/sites/default/files/documents/public_events/robocalls-all-rage-ftc-summit/robocallsummittranscript.pdf).

caller ID information. The telephone network has its origins in a manual switchboard that allowed a human operator to make connections between two known entities.<sup>28</sup> A small group of well-known carriers were in control and were highly regulated.<sup>29</sup> Placing calls took significant time and money, and callers could not easily conceal their identities.<sup>30</sup>

Now, anyone can build a viable telephone services business wherever there is an Internet connection.<sup>31</sup> As a result, the number of service providers has grown exponentially and now includes thousands of small companies all over the world.<sup>32</sup> In addition, VoIP technology allows consumers to enjoy high-quality phone calls with people on the other side of the globe for an affordable price.<sup>33</sup> With this efficiency came other changes: instead of a voice path between one wire pair, the call travels as data; identifying information can be spoofed; many different players are involved in the path of a single call; and the distance between the endpoints is not particularly important.<sup>34</sup> As a result, it is not only much cheaper to blast out robocalls; it is also easier to hide one's identity when doing so.

#### **1. New Technologies Have Made Robocalls Extremely Inexpensive**

Until recently, telemarketing required significant capital investment in specialized hardware and labor.<sup>35</sup> Now, robocallers benefit from automated dialing technology, inexpensive

---

<sup>28</sup> Bellovin, Tr. at 12.

<sup>29</sup> Schulzrinne, Tr. at 22; Rupy, Tr. at 46-47; Diggs, Tr. at 55.

<sup>30</sup> Bellovin, Tr. at 12-17.

<sup>31</sup> Herman, Tr. at 60-61; Maxson, Tr. at 96.

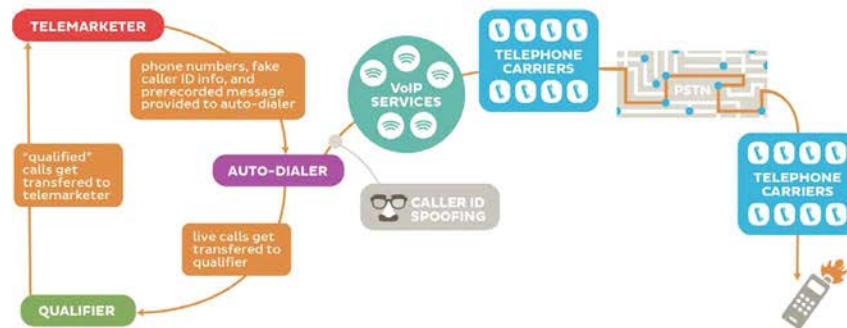
<sup>32</sup> Schulzrinne, Tr. at 22.

<sup>33</sup> See, e.g., Bellovin, Tr. at 16-17.

<sup>34</sup> *Id.* at 17.

<sup>35</sup> Hermann, Tr. at 58-59; Schulzrinne, Tr. at 24.

long distance calling rates, and the ability to move internationally and employ cheap labor.<sup>36</sup> The only necessary equipment is a computer connected to the Internet.<sup>37</sup> The result: law-breaking telemarketers can place robocalls for less than one cent per minute. In addition, the cheap, widely available technology has resulted in a proliferation of entities available to perform any portion of the telemarketing process, including generating leads, placing automated calls, gathering consumers' personal information, or selling products.<sup>38</sup> Because of the dramatic decrease in upfront capital investment and marginal cost, robocallers – like email spammers – can make a profit even if their contact rate is very low.<sup>39</sup>



*Technology enables a cheap and scalable model for robocalls.*<sup>40</sup>

<sup>36</sup> Schulzrinne, Tr. at 24.

<sup>37</sup> Hermann, Tr. at 59-61.

<sup>38</sup> Schulzrinne, Tr. at 20-21; Maxson, Tr. at 95-98.

<sup>39</sup> Schulzrinne, Tr. at 21; Bellovin, Tr. at 16-17.

<sup>40</sup> The PSTN is the "Public Switched Telephone Network." It consists of transmission facilities (e.g., phone lines, fiber optic cables, microwave transmission links, cellular radios, communication satellites, etc.) and switching facilities (central office switches, databases for 800 number translation, gear for cellular handoffs, multiplexors, etc.).

## 2. New Technologies Have Made It Easier for Robocallers to Hide

Technological changes have also affected the marketplace by enabling telemarketers to conceal their identities when they place calls. First, direct connections do not exist between every pair of carriers, so intermediate carriers are necessary to connect the majority of calls. Thus, the typical call now takes a complex path, traversing the networks of multiple VoIP and legacy carriers before reaching the end user.<sup>41</sup> Each of these carriers knows which carrier passed a particular phone call onto its network, but likely knows little else about the origin of the call.<sup>42</sup> Such a path makes it cumbersome to trace back to a call's inception.<sup>43</sup> All too often, this process to trace the call fails completely because one of the carriers in the chain has not retained the records that would further an investigation.<sup>44</sup>

Second, new technologies allow callers to easily manipulate the caller ID information that appears with an incoming phone call.<sup>45</sup> While "caller ID spoofing" has some beneficial uses,<sup>46</sup> it also allows robocallers to deceive consumers by pretending to be an entity with a local phone number or a trusted institution such as a bank or government agency.<sup>47</sup> In addition, robocallers can change their phone numbers frequently in an attempt to avoid detection.<sup>48</sup>

---

<sup>41</sup> Panagia, Tr. at 130-32; Bellovin, Tr. at 17.

<sup>42</sup> Panagia, Tr. at 132; Maxson, Tr. at 100.

<sup>43</sup> Schulzrinne, Tr. at 24-25; Maxson, Tr. at 100; Bash, Tr. at 104.

<sup>44</sup> Panagia, Tr. at 160-61; *see also id.* at 132-133; Schulzrinne, Tr. at 21.

<sup>45</sup> Schulzrinne, Tr. at 24-26.

<sup>46</sup> *See, e.g.,* Panagia, Tr. at 129 (AT&T allows the third party that performs AT&T's customer service to "spoof" AT&T's customer service line).

<sup>47</sup> Schulzrinne, Tr. at 21-22.

<sup>48</sup> *Id.* at 24-26; Maxson, Tr. at 97; Bash, Tr. at 103. Under the Truth in Caller ID Act, it is generally illegal to transmit misleading or inaccurate caller ID information with intent to defraud. *See*



Finally, new technologies allow robocallers to operate outside of jurisdictions where they are most likely to face prosecution.<sup>49</sup> Indeed, all of the many different entities involved in the path of a robocall can be located in different countries, making investigations even more challenging.



*The path of a robocall can span the globe.*

Truth in Caller ID Act, 47 U.S.C. § 227(e); cf. 16 C.F.R. Part 310.4(a)(8) (the Telemarketing Sales Rule requires that sellers and telemarketers transmit or cause to be transmitted the telephone number and, when made available by the telemarketer's carrier, the name of the telemarketer, to any caller identification service in use by a recipient of a telemarketing call, or transmit the customer service number of the seller on whose behalf the call is made and, when made available by the telemarketer's seller, the name of the seller. Under this provision, it is not necessary to prove intent to defraud.)).

<sup>49</sup> Schulzrinne, Tr. at 21; Bellovin, Tr. at 16-17.

## **B. Need to Stimulate Technological Solutions**

### **1. Robocall Contests**

Recognizing the need to spur the marketplace into developing technical solutions that protect American consumers from illegal robocalls, the FTC held its first public contest in October 2012, offering a \$50,000 prize to the individual or small team who proposed the best technological solution that blocks robocalls on consumers' landlines and mobile phones. After reviewing 798 submissions, the FTC announced three winning solutions on April 2, 2013.<sup>50</sup> Six months later, one of the solutions, Nomorobo, was made available to consumers, and it now reports having over 170,000 subscribers<sup>51</sup> and has blocked over 24 million robocalls.<sup>52</sup> Following on the success of the first challenge, the FTC conducted its second contest, "Zapping Rachel," in August 2014, offering \$17,000 in prizes focused on the open source advancement of honeypot design.<sup>53</sup> Zapping Rachel challenged contestants to build a more advanced honeypot, identify vulnerabilities in an existing honeypot, and analyze data from a honeypot. The FTC

---

<sup>50</sup> See Press Release, FTC Announces Robocall Challenge Winners; Proposals Would Use Call Filter Software to Reduce Illegal Calls (Apr. 2, 2013), *available at* <http://www.ftc.gov/opa/2013/04/robocall.shtm>.

<sup>51</sup> See Alina Tugend, *A Year Fighting Robocalls, and Finding the Right Parts*, N.Y. TIMES, Dec. 26, 2014, *available at* [http://www.nytimes.com/2014/12/27/your-money/a-year-of-shortcuts-the-fight-against-robocalls-gains-ground.html?\\_r=0](http://www.nytimes.com/2014/12/27/your-money/a-year-of-shortcuts-the-fight-against-robocalls-gains-ground.html?_r=0).

<sup>52</sup> See Nomorobo Home Page, <https://www.nomorobo.com/> (last visited June 2, 2015).

<sup>53</sup> In 2012, the FTC launched its robocall honeypot – a group of phone lines that amasses information on robocalls, such as the date and time the honeypot receives the robocall and a recording of the robocall. The FTC utilizes the honeypot to collect evidence against robocallers and facilitate a more rapid law enforcement response.



held Zapping Rachel at DEF CON 22, one of the most established conferences for information security experts, and announced five winners on August 28, 2014.<sup>54</sup>

The FTC is conducting two new robocall contests this summer: DetectaRobo and Robocalls: Humanity Strikes Back. DetectaRobo was held in conjunction with the 2015 National Day of Civic Hacking on June 6-7, 2015, and asked contestants to analyze data from a honeypot and create predictive algorithms that identify robocalls.<sup>55</sup> Robocalls: Humanity Strikes Back will be held in two phases with the final phase taking place at DEF CON 23, August 5-9, 2015. It challenges contestants to build solutions that not only block robocalls from reaching consumers, but enable consumers to forward those unwanted robocalls to a crowd-source honeypot so that law enforcement and industry stakeholders can use the data collected.<sup>56</sup> The FTC anticipates that the 2015 robocall contests will continue to encourage private sector development of new technologies that will advance the fight against robocalls and foster new industry partners.

## **2. Coordinating with Technical Experts, Industry, and Other Stakeholders**

Since 2012, in addition to stimulating technological developments through public challenges, the FTC also has engaged with technical experts, academics, and others through industry groups, such as the Messaging, Malware and Mobile Anti-Abuse Working Group

<sup>54</sup> See Press Release, FTC Announces Winners of “Zapping Rachel” Robocall Contest (Aug. 28, 2014), available at <https://www.ftc.gov/news-events/press-releases/2014/08/ftc-announces-winners-zapping-rachel-robocall-contest>.

<sup>55</sup> See Fed. Trade Comm’n, DetectaRobo, <https://www.ftc.gov/detectarobo> (last visited June 2, 2015); Press Release, FTC Announces New Robocall Contests to Combat Illegal Automated Calls (Mar. 4, 2015), available at <https://www.ftc.gov/news-events/press-releases/2015/03/ftc-announces-new-robocall-contests-combat-illegal-automated>.

<sup>56</sup> See Fed. Trade Comm’n, Robocalls: Humanity Strikes Back, <https://www.ftc.gov/strikeback> (last visited June 2, 2015); Press Release, FTC Announces New Robocall Contests to Combat Illegal Automated Calls (Mar. 4, 2015), available at <https://www.ftc.gov/news-events/press-releases/2015/03/ftc-announces-new-robocall-contests-combat-illegal-automated>.

(“M<sup>3</sup>AAWG”). M<sup>3</sup>AAWG is a consortium of industry, regulators, and academics focused on developing solutions to mitigate various forms of messaging abuse such as email spam.<sup>57</sup> After discussions with the FTC and others, M<sup>3</sup>AAWG leadership formed the Voice and Telephony Abuse Special Interest Group (“VTA SIG”) in 2014, a subgroup formed to apply M<sup>3</sup>AAWG’s expertise on messaging abuse to voice spam, such as robocalls.<sup>58</sup>

Through the VTA SIG, the FTC coordinates with experts working on industry standards that will combat caller ID spoofing by enabling the authentication of VoIP calls, such as the Internet Engineering Task Force’s working group called “STIR” – Secure Telephone Identity Revisited.<sup>59</sup> The FTC further promotes technical advancements by collaborating with its counterparts in other countries, through its leadership in the London Action Plan (“LAP”), an international syndicate of government agencies and private sector representatives focused on international spam enforcement cooperation.<sup>60</sup> In fact, LAP, M<sup>3</sup>AAWG, and VTA SIG are currently meeting in Dublin, Ireland. The FTC is taking a leadership role in facilitating LAP’s enforcement initiatives and organizing and running these conferences.

### 3. Policies to Facilitate Market Solutions

The Commission has long recognized the need for policies that facilitate the development of technological products. In January 2015, FTC staff submitted a response to the FCC’s request for public comment on whether there are legal or regulatory prohibitions that prevent telephone

---

<sup>57</sup> See M<sup>3</sup>AAWG, Activities, <https://www.m3aawg.org/> (last visited June 2, 2015).

<sup>58</sup> See M<sup>3</sup>AAWG, Voice and Telephony Abuse Special Interest Group, [https://www.m3aawg.org/vta-sig#About\\_VTASIG](https://www.m3aawg.org/vta-sig#About_VTASIG) (last visited June 2, 2015).

<sup>59</sup> See Internet Eng’g Task Force, Secure Telephone Identity Revisited (STIR), <https://datatracker.ietf.org/wg/stir/charter/> (last visited June 2, 2015).

<sup>60</sup> See London Action Plan, <http://londonactionplan.org/> (last visited June 2, 2015).

carriers from offering call-blocking technology.<sup>61</sup> The FTC staff comment outlined the vital need for call-blocking technologies as an integral component to providing subscribers with relief from illegal unwanted calls, and indicated its view that no legal impediments existed to prevent the provision of such services to subscribers.<sup>62</sup>

### III. Consumer Education

Public education is also an essential tool in the FTC's consumer protection and fraud prevention work. The Commission's education and outreach program reaches tens of millions of people a year through our website, the media, and partner organizations that disseminate consumer information on the FTC's behalf.

The FTC delivers practical, plain language information on numerous issues. The Commission also uses law enforcement announcements as opportunities to remind consumers how to recognize a similar situation and report it to the FTC. In the case of robocalls, whether the offer involves fraudulent credit card services, so-called auto warranty protection plans, or bogus vacation travel packages, the FTC's message to consumers is simple: if you answer a call and hear an unwanted recorded sales message – hang up. Period. Other key messages to

<sup>61</sup> Fed. Comm'n Comm'n, Consumer and Governmental Affairs Bureau Seeks Comment on Robocalls and Call-Blocking Issues Raised by the National Association of Attorneys General on Behalf of Thirty-Nine Attorneys General, DA 14-1700 (Nov. 24, 2014), *available at* <https://www.fcc.gov/document/cgb-seeks-comment-call-blocking-letter-attorneys-general>.

<sup>62</sup> See Fed. Trade Comm'n, FTC Staff Comment Before the Federal Communications Commission on Public Notice DA 14-1700, Regarding the Issues Relating to Carrier Implementation of Call-Blocking Technology (Jan. 23, 2015), *available at* <https://www.ftc.gov/policy/policy-actions/advocacy-filings/2015/01/ftc-staff-comment-federal-communications-commission>. On May 27, 2015, FCC Chairman Wheeler announced a proposal for the FCC to crack down on unwanted robocalls and text messages, which will be voted on by the FCC Commission on June 18. The proposal encourages robocall-blocking technologies and clarifies that carriers can, and should, offer consumers robocall-blocking tools. Fed. Comm'n Comm'n, Another Win For Consumers, <https://www.fcc.gov/blog/another-win-consumers> (May 27, 2015, 14:28 EDT); Fed. Comm'n Comm'n, Fact Sheet on Consumer Protection Proposal (May 27, 2015), *available at* <https://www.fcc.gov/document/fact-sheet-consumer-protection-proposal>.

consumers include how to place a phone number on the Do Not Call Registry, what to consider before asking a phone carrier to block calls, and how and where to report illegal robocalls.<sup>63</sup> The FTC’s education materials also explain how robocallers use technology to make thousands of calls at minimal cost, send fake caller ID information, and conceal their locations. The FTC disseminates these tips through articles,<sup>64</sup> blog posts,<sup>65</sup> social media,<sup>66</sup> infographics,<sup>67</sup> videos,<sup>68</sup> audio,<sup>69</sup> and campaigns such as “Pass It On” – an innovative means of arming older consumers with information about scams that they can “pass on” to their friends and family members.<sup>70</sup>

The FTC updates its consumer education whenever it has new information to share. The Commission’s library of articles on robocall scams in English and Spanish also includes pieces describing credit card interest rate reduction scams, auto service contract and warranty fraud, and

---

<sup>63</sup> See, e.g., National Do Not Call Registry, <http://www.consumer.ftc.gov/articles/0108-national-do-not-call-registry> (last visited June 2, 2015).

<sup>64</sup> See, e.g., FTC Robocall Microsite, <http://www.consumer.ftc.gov/features/feature-0025-robocalls> (last visited June 2, 2015).

<sup>65</sup> See, e.g., FTC Consumer Information Blog, <http://www.consumer.ftc.gov/blog> (last visited June 2, 2015); Bikram Bandy, Your top 5 Questions about unwanted calls and the National Do Not Call Registry (Mar. 9, 2015), <http://www.consumer.ftc.gov/blog/your-top-5-questions-about-unwanted-calls-and-national-do-not-call-registry>.

<sup>66</sup> See, e.g., FTC Robocalls Facebook Q&A Transcript (Oct. 25, 2012), <https://www.ftc.gov/sites/default/files/attachments/ftc-facebook-chats/1210robocallschallenge-fb.pdf>.

<sup>67</sup> See, e.g., FTC Robocalls Infographic, [https://www.ftc.gov/sites/default/files/documents/public\\_events/robocalls-all-rage-ftc-summit/pdf-0113-robocalls-infographic.pdf](https://www.ftc.gov/sites/default/files/documents/public_events/robocalls-all-rage-ftc-summit/pdf-0113-robocalls-infographic.pdf).

<sup>68</sup> See, e.g., FTC Video and Media, <http://www.consumer.ftc.gov/media> (last visited June 2, 2015).

<sup>69</sup> See, e.g., FTC Consumer Information Audio, “Hang Up on Robocalls,” <http://www.consumer.ftc.gov/media/audio-0045-hang-robocalls> (last visited June 2, 2015).

<sup>70</sup> See Pass It On, <http://www.consumer.ftc.gov/features/feature-0030-pass-it-on#identity-theft> (last visited June 2, 2015).



travel-related schemes.<sup>71</sup> When Robocall Challenge participants submitted to the Commission techniques they were using to successfully reduce illegal robocalls, the GSA and FTC used these tips in a video with consumer suggestions about stopping unwanted robocalls.<sup>72</sup>

#### IV. Next Steps and Conclusion

The Do Not Call Registry remains enormously successful in protecting consumers against unsolicited calls from legitimate telemarketers. But, as technology changes and fraudsters exploit those changes, we must remain agile and creative. The Commission will continue its multifaceted efforts to fight illegal robocalls, including the following actions:

- Continue Aggressive Law Enforcement
  - We will maintain our enforcement efforts, in coordination with state, federal, and international partners, to target high-volume offenders and pursue robocall gatekeepers in order to stop the largest number of illegal calls.
  - We will work with the telecommunications industry, encouraging carriers to be proactive in monitoring for illegal robocalls and securing the information necessary for prosecutions.
- Spur Innovation
  - We will work with industry leaders and other experts to further stimulate the development of technological solutions to protect consumers from illegal robocalls.
  - We will continue to encourage industry-wide coordination to create and deploy VoIP standards that incorporate robust authentication capabilities. Such

<sup>71</sup> See FTC Consumer Information, “Travel Tips” (May 2013), <http://www.consumer.ftc.gov/articles/0046-travel-tips>; FTC Consumer Information, “Auto Service Contracts and Warranties” (Aug. 2012), <http://www.consumer.ftc.gov/articles/0054-auto-service-contracts-and-warranties>; FTC Consumer Information, “Credit Card Interest Rate Reduction Scams” (Feb. 2011), <http://www.consumer.ftc.gov/articles/0131-credit-card-interest-rate-reduction-scams>; see generally FTC Robocall Microsite, <http://www.consumer.ftc.gov/features/feature-0025-robocalls> (last visited June 2, 2015); FTC Robocall Microsite in Spanish, “Llamadas automáticas pregrabadas o robocalls,” <http://www.consumidor.ftc.gov/destacado/destacado-s0025-llamadas-automaticas-pre-grabadas-o-robocalls> (last visited June 2, 2015).

<sup>72</sup> Robocall Challenge: Consumer Tips & Tricks (Apr. 2, 2013), <http://www.consumer.ftc.gov/media/video-0086-robocall-challenge-consumer-tips-tricks>.

coordination is the only way to ensure a future phone system with accurate and truthful calling information.

- Engage in Ongoing Consumer Education
  - We will continue our broad outreach to consumers regarding the Do Not Call Registry as well as illegal robocalls and how best to fight them.
- Work with Congress
  - We stand ready to assist in your efforts to protect consumers.

Thank you for the opportunity to share some of the highlights regarding the FTC's battle against illegal robocalls. We look forward to working with you on this important issue.

**Overview of Statements of Attorney General Chris Koster  
Special Committee on Aging Panel Discussion  
June 10, 2015  
Washington, D.C.**

I take this opportunity on behalf of Missouri Attorney General Chris Koster to thank Chairwoman Senator Susan Collins and my friend and ranking committee member Senator Claire McCaskill for inviting us here this afternoon.

Missouri's No-Call Law

The Missouri Attorney General's Office has a division dedicated to responding to complaints from Missouri consumers. The Consumer Protection Division receives complaints about a wide variety of scams and fraud, such as illegal debt collecting practices, and identity theft. However, the *number one* complaint of Missourians—by a significant margin—is about unwanted and illegal telemarketing calls. In 2014 alone, our office received more than 57,000 complaints, 52,000+ of which were about telemarketing calls. The next highest category of complaint—about debt collectors—had just over 1,200 complaints.

As in most states, Missouri's No-Call Law allows individuals who do not want to be called by telemarketers to register their residential and cell phone numbers on the No-Call List.

The law prohibits telemarketers from calling those individuals who have been added to the list, with some exceptions that have been written into the law. Specifically, the No-Call Law prohibits any person or entity from making or causing to be made “telephone solicitations” to any residential subscriber in the State of Missouri who has given notice to the Attorney General of such subscriber’s objection to receiving telephone solicitations. MO.REV.STAT. § 407.1098.

There are several exceptions to the definition of “telephone solicitation,” which act as exceptions to the No-Call Law. Pursuant to § 407.1095(3)(a)-(d), the following calls are exempt from prosecution:

- (a) calls to residential subscribers with the subscriber’s “prior express invitation or permission”;
- (b) by or on behalf of any entity with whom a residential subscriber has had a business contact within the past 180 days or a current business or personal relationship;
- (c) by or on behalf of any entity organized pursuant to Chapter 501(c)(3) of the United States Internal Revenue Code, while such entity is engaged in fund-raising to support the charitable purpose for which the entity was established;
- (d) By or on behalf of any entity over which a federal agency has regulatory authority to the extent that the entity is required to



maintain a license, permit or certificate to sell or provide the merchandise being offered AND the entity is required by law or rule to develop and maintain a no-call list.

#### Overview of Complaints

Every day our No-Call Unit receives complaints from people – many of whom are seniors – who have been abused or harassed by telemarketers who have no respect for the law or the privacy of those whom they victimize.

Just last month our office received a complaint from an 80-year-old woman in St. Louis. She had received a call from someone telling her that she is eligible for a back brace paid for by Medicare. The caller was able to get the woman's Medicare identification number – which is her social security number – and her date of birth. After hanging up the phone she quickly realized that something was not right with that call and she notified our office.

We also frequently receive complaints about robocalls, many of which specifically target seniors. For example, one recorded message making the rounds informs the senior consumer that he or she is eligible for a free medical alert bracelet, if the senior will simply provide their identifying information.

While some technologies, such as caller ID, help address unwanted calls, even then technologies may be exploited. For example, caller ID

spoofing happens when a caller deliberately falsifies the name and telephone number appearing on the caller ID information to disguise the caller's true identity.

One of the most frequent spoofing complaints our office receives from seniors is that their caller ID relays the letters S – S – I ("SSI") as the caller's identity. The seniors believe the call to be from the Social Security Administration. However, upon answering the call, the consumer is immediately asked survey questions designed to elicit personal information.

The Missouri No-Call Law specifically targets spoofing. The Missouri statute provides that "[n]o person or entity who makes a telephone solicitation to a residential subscriber in this state shall knowingly use any method to block or otherwise circumvent any subscriber's use of a caller identification service." Mo.Rev.Stat. § 407.1104.2

#### Litigation

Our office is fighting back in the courtroom. In 2014, we obtained more than \$600,000 in judgments penalizing telemarketers for their illegal conduct and filed 20 cases against telemarketers across the United States that violated Missouri law. Significantly, our office obtained court orders permanently prohibiting 28 telemarketers from ever placing another call into the State of Missouri. But they are clever and they are relentless. Unfortunately, it often becomes as frustrating as the old arcade game "whack

a mole.” We shut them down and they pop up again in other states or with different identities. Many have resorted to setting up shop and making calls from overseas locations, effectively nullifying our ability to obtain enforcement jurisdiction over them.

#### Looking Forward

This is a battle, however, which must be fought on many fronts. We need the help of private industry, including the telephone service providers, to create solutions to permanently stop unwanted telemarketing calls.

Already technologies exist to reduce the number of robocalls to consumers’ phones. These “call blockers” filter incoming telemarketing calls before they reach consumers’ phones, thus dramatically reducing the number of unwanted calls a person receives. Yet, the major phone carriers have resisted allowing their customers to have access to these call blocking technologies, claiming that federal law prohibits it.

To quote from a U.S. Telecom representative at a July 10, 2013 Senate Subcommittee Consumer Protection Hearing:

“The Current legal framework simply does not allow  
[phone companies] to decide for the consumer which calls  
should be allowed to go through and which should be  
blocked.”

If so, then that should be changed. If that is the only thing stopping them, then by all means, we should clarify the law and give them such power.

That is why last fall, Missouri Attorney General Chris Koster and Indiana Attorney General Greg Zoeller, joined by 37 other attorneys general, penned and submitted a letter to the Federal Communications Commission urging the Commission to allow phone companies to utilize call-blocking technologies that would better protect consumers from unwanted calls and scams. That letter is attached to my written testimony as exhibit A.

We are thankful and encouraged by the fact that FCC Chairman Wheeler agrees. In response to the letter, Chairman Wheeler submitted a proposal to protect Americans from unwanted robocalls, spam text messages, and telemarketing calls. It looks like the FCC will, in fact, provide clarity on the issue based on Chairman Wheeler's request. The proposal will be voted on at the Commission's Open Meeting on June 18, 2015. I have also attached to my testimony as exhibit B a copy of a news release regarding Chairman Wheeler's response to Attorney General Koster's letter. We cannot emphasize enough the importance of what the FCC is hopefully about to do. It is right for our citizens. It is especially right for our elderly, which is what this commission is all about. We urge the Commission to pass the proposal.

Our office is encouraged by the progress we have made, but we recognize the continuing challenges that need to be addressed. Consumers

have made it clear that they are fed up with the number of unwanted telemarketing calls they receive. We must continue to research and employ newer technologies to help in our efforts to keep up with the illegal robocallers. The telephone carriers are in the unique position to help their own customers block these calls. Once the major telephone carriers are on board, we can truly make a difference in the lives of consumers by giving THEM the power to stop illegal telemarketing phone calls at their inception.

While we do not share the industry's interpretation of the existing rule of law, to the extent that there is any ambiguity regarding phone company's legal authority to honor its customer's request that they block these unwanted calls before they arrive at their personal telephone, we would request clarity on the issue.

Thank you again for the opportunity to briefly testify before you this afternoon and for your time and attention on this important matter.



---

---

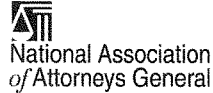
## **Statements for the Record**

---

---







PRESIDENT  
Jim Hood  
*Mississippi Attorney General*

PRESIDENT-ELECT  
Marty Jackley  
*South Dakota Attorney General*

VICE PRESIDENT  
George Jepsen  
*Connecticut Attorney General*

IMMEDIATE PAST PRESIDENT  
J.B. Van Hollen  
*Wisconsin Attorney General*

EXECUTIVE DIRECTOR  
James McPherson

Exhibit A

September 9, 2014

The Honorable Tom Wheeler  
Chairman  
Federal Communications Commission  
445 12<sup>th</sup> Street, S.W.  
Washington, D.C. 20554

Dear Chairman Wheeler,

The undersigned Attorneys General, on behalf of the millions of Americans regularly receiving unwanted and harassing telemarketing calls, formally request an opinion from the Federal Communications Commission (the "FCC") regarding telephone carriers' legal ability to implement call-blocking technology.

#### I. Background

On July 10, 2013, the U.S. Senate's Subcommittee on Consumer Protection, Product Safety, and Insurance (the "Subcommittee") held a hearing entitled "Stopping Fraudulent Robocall Scams: Can More Be Done?" During that hearing, representatives from US Telecom Association and CTIA-The Wireless Association testified that legal barriers prevented carriers from implementing advanced call-blocking technology to reduce the number of unwanted telemarketing calls. Examples of blocking technologies currently available include "NoMoRobo" for VOIP phones, developed by Aaron Foss, winner of the FTC's \$50,000 Robocall Challenge; "Call Control" for smart phones, developed by the Kedlin Company; and "Telemarketing Guard," developed by Primus Telecommunications Canada, Inc. for Canadian consumers. American consumers should not have to seek out piecemeal solutions—instead, carriers should make solutions more easily accessible to consumers.

During prepared statements at the 2013 hearing, the US Telecom representative stated:

"First, under existing laws . . . phone companies have a legal obligation to complete phone calls. These companies may not block or otherwise prevent phone calls from transiting their networks or completing such calls. The current legal framework simply does not allow [phone companies] to decide for the consumer which calls should be allowed to go through and which should be blocked."

2030 M Street, NW  
Eighth Floor  
Washington, DC 20036  
Phone: (202) 326-6000  
<http://www.naag.org/>

Thereafter, on August 16, 2013, Senator Claire McCaskill, chairwoman of the Subcommittee, sent a letter to the heads of US Telecom and CTIA-The Wireless Association. In this letter, Senator McCaskill asked for a “complete analysis of the challenges your industry foresees in implementing” call-blocking technologies.

On October 15, 2013, US Telecom responded to Senator McCaskill. In its response, US Telecom claimed that its members are subject to legacy common-carrier regulation and enforcement of the regulations by the FCC. US Telecom also alleged that “the FCC has concluded that call blocking is an unjust and unreasonable practice under section 201(b) of the Communications Act of 1934.” Indeed, US Telecom stated that if a phone carrier engages in call blocking, the FCC can assess a forfeiture of as much as \$150,000 for each violation, up to a total \$1,500,000 statutory maximum for a single act or failure to act.

Because solutions like NoMoRobo, Call Control, and Telemarketing Guard are call-blocking technologies, US Telecom concluded that the current legal framework prohibits its members from using them to protect their customers from unwanted robocalls.

## II. Request of the Attorneys General

State law enforcement officials are doing everything possible to track down and prosecute those that engage in illegal telemarketing. However, law enforcement cannot fight this battle alone. Call-blocking technology like NoMoRobo, Call Control, and Telemarketing Guard appears to be the first major advancement towards a solution.

Nonetheless, the telephone companies’ resistance to embrace call-blocking technology, as evidenced by US Telecom’s response to Senator McCaskill, raises important questions. If a solution to the nation’s illegal telemarketing problem is possible, it will require the private sector—including telephone carriers—to get involved. To that end, we respectfully request a formal opinion from the FCC on the following issues:


- (1) What *legal and/or regulatory* prohibitions, if any, prevent telephone carriers from implementing call-blocking technology such as NoMoRobo, Call Control, and Telemarketing Guard? Does the answer change if the telephone companies’ customers affirmatively “opt into” the call-blocking technology (either for a fee or as a free service)?
- (2) US Telecom claims that telephone carriers “can and do block harassing and annoying telephone traffic at their end-user customer’s request,” but only for a “discrete set of specific phone numbers.” At a customer’s request, can telephone carriers legally block certain types of calls (*e.g.*,


telemarketing calls) if technology is able to identify incoming calls as originating or probably originating from a telemarketer?

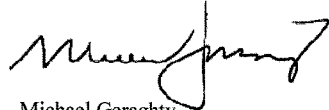
- (3) US Telecom describes the FCC's position as "strict oversight in ensuring the unimpeded delivery of telecommunications traffic." Is US Telecom's characterization of the FCC's position accurate? If so, upon what basis does the FCC claim that telephone carriers may not "block, choke, reduce or restrict telecommunications traffic in any way"?

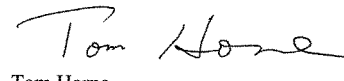
Thank you for your consideration on this matter. Hopefully, we can all work cooperatively to find a solution to the unwanted telemarketing problem in the United States.

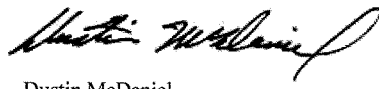
Respectfully,

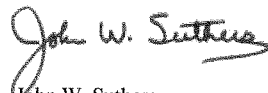
  
Greg Zoeller  
Indiana Attorney General

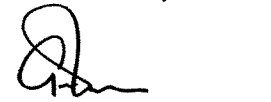
  
Chris Koster  
Missouri Attorney General

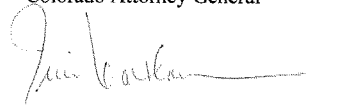
  
Michael Geraghty  
Alaska Attorney General

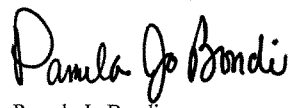
  
Tom Horne  
Arizona Attorney General


  
Dustin McDaniel  
Arkansas Attorney General

  
John W. Suthers  
Colorado Attorney General

  
George Jepsen  
Connecticut Attorney General

  
Irvin Nathan  
District of Columbia Attorney General

  
Pamela Jo Bondi  
Florida Attorney General

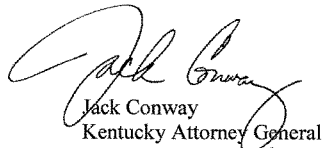
  
Lenny Rapadas  
Guam Attorney General



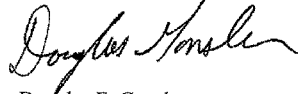
David Louie  
Hawaii Attorney General



Lisa Madigan  
Illinois Attorney General



Jack Conway  
Kentucky Attorney General



Douglas F. Gansler  
Maryland Attorney General



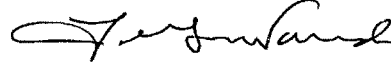
Lori Swanson  
Minnesota Attorney General



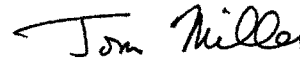
Tim Fox  
Montana Attorney General



Joseph Foster  
New Hampshire Attorney General



Lawrence Wasden  
Idaho Attorney General



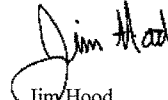
Tom Miller  
Iowa Attorney General



Janet Mills  
Maine Attorney General



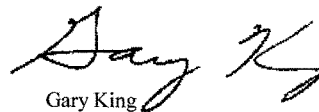
Bill Schuette  
Michigan Attorney General



Jim Hood  
Mississippi Attorney General



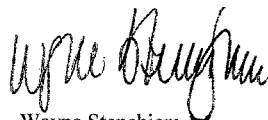
Catherine Cortez Masto  
Nevada Attorney General



Gary King  
New Mexico Attorney General



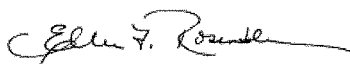
Roy Cooper  
North Carolina Attorney General



Wayne Stenehjem  
North Dakota Attorney General



Mike DeWine  
Ohio Attorney General



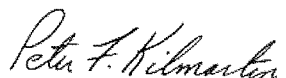
Ellen F. Rosenblum  
Oregon Attorney General




Kathleen Kane  
Pennsylvania Attorney General



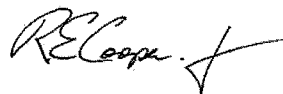
César R. Miranda Rodríguez  
Puerto Rico Attorney General



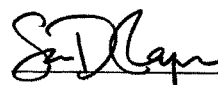
Peter Kilmartin  
Rhode Island Attorney General



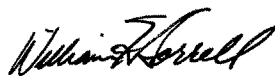
Marty Jackley  
South Dakota Attorney General



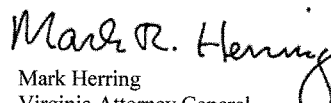
Robert E. Cooper, Jr.  
Tennessee Attorney General



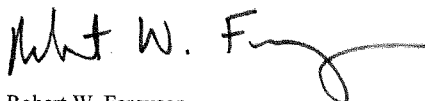
Sean Reyes  
Utah Attorney General



William H. Sorrell  
Vermont Attorney General



Mark Herring  
Virginia Attorney General



Robert W. Ferguson  
Washington Attorney General



Patrick Morrisey  
West Virginia Attorney General



Peter K. Michael  
Wyoming Attorney General

**2015 NEWS ARCHIVES**

**FCC Commissioner endorses AG Koster's request to allow phone companies to block telemarketing calls**  
May 28, 2015, 15:22 PM

**Jefferson City, Mo.** – In response to Attorney General Koster's efforts, the chairman of the Federal Communications Commission (FCC) has submitted a proposal to protect Americans from unwanted robocalls, spam text messages, and telemarketing calls. Koster today encouraged FCC members to pass the proposal, and allow phone companies to utilize call-blocking technologies to better protect consumers from unwanted calls and scams.

Last September, Koster and Indiana Attorney General Greg Zoeller submitted a **letter** signed by 37 other state and territorial attorneys general to the FCC urging the commission to recognize call-blocking filters as legally allowable, if requested by customers. The FCC will vote on the chairman's proposal at the Commission's Open Meeting on June 18, 2015.

"Missouri's no-call law has been very effective, but newer technologies enable unwanted callers to place hundreds or even thousands of robocalls in an instant. I urge the FCC to allow phone companies to offer customers a way to block unwanted calls," Koster said.

Koster said his office received more than 52,000 complaints last year about unwanted calls, a majority of which were robocalls.

Koster reminds Missourians they can sign up for the Do-Not-Call hotline on his [website](#) or by calling **1-866-662-2551**. He encourages consumers who receive harassing solicitation calls to [file a complaint](#) at **1-866-buzzoff (1-866-289-9633)**.