AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. HRG. 113–117

STOPPING FRAUDULENT ROBOCALL SCAMS: CAN MORE BE DONE?

HEARING

BEFORE THE

SUBCOMMITTEE ON CONSUMER PROTECTION, PRODUCT SAFETY, AND INSURANCE

OF THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION
UNITED STATES SENATE

ONE HUNDRED THIRTEENTH CONGRESS

FIRST SESSION

JULY 10, 2013

Printed for the use of the Committee on Commerce, Science, and Transportation

U.S. GOVERNMENT PRINTING OFFICE

85–765 PDF WASHINGTON : 2013

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED THIRTEENTH CONGRESS

FIRST SESSION

JOHN D. ROCKEFELLER IV, West Virginia, *Chairman*

BARBARA BOXER, California
BILL NELSON, Florida
MARIA CANTWELL, Washington
MARK PRYOR, Arkansas
CLAIRE McCASKILL, Missouri
AMY KLOBUCHAR, Minnesota
MARK WARNER, Virginia
MARK BEGICH, Alaska
RICHARD BLUMENTHAL, Connecticut
BRIAN SCHATZ, Hawaii
WILLIAM COWAN, Massachusetts
MARTIN HEINRICH, New Mexico

JOHN THUNE, South Dakota, *Ranking*
ROGER F. WICKER, Mississippi
ROY BLUNT, Missouri
MARCO RUBIO, Florida
KELLY AYOTTE, New Hampshire
DEAN HELLER, Nevada
DAN COATS, Indiana
TIM SCOTT, South Carolina
TED CRUZ, Texas
DEB FISCHER, Nebraska
RON JOHNSON, Wisconsin
JEFF CHIESA, New Jersey

ELLEN L. DONESKI, *Staff Director*
JAMES REID, *Deputy Staff Director*
JOHN WILLIAMS, *General Counsel*
DAVID SCHWIETERT, *Republican Staff Director*
NICK ROSSI, *Republican Deputy Staff Director*
REBECCA SEIDEL, *Republican General Counsel and Chief Investigator*

SUBCOMMITTEE ON CONSUMER PROTECTION, PRODUCT SAFETY, AND INSURANCE

CLAIRE McCASKILL, Missouri, *Chairman*
BARBARA BOXER, California
MARK PRYOR, Arkansas
AMY KLOBUCHAR, Minnesota
RICHARD BLUMENTHAL, Connecticut
BRIAN SCHATZ, Hawaii
WILLIAM COWAN, Massachusetts

DEAN HELLER, Nevada, *Ranking Member*
ROY BLUNT, Missouri
KELLY AYOTTE, New Hampshire
DAN COATS, Indiana
TED CRUZ, Texas
DEB FISCHER, Nebraska

CONTENTS

	Page
Hearing held on July 10, 2013	1
Statement of Senator McCaskill	1
Statement of Senator Heller	3
Statement of Senator Pryor	38

WITNESSES

Lois Greisman, Associate Director, Division of Marketing Practices, Bureau of Consumer Protection, Federal Trade Commission	4
Prepared statement	6
Eric J. Bash, Associate Chief, Enforcement Bureau, Federal Communications Commission	18
Prepared statement	20
Kevin Rupy, Senior Director, Law and Policy, United States Telecom Association	32
Prepared statement	33
Michael F. Altschul, Senior Vice President and General Counsel, CTIA—The Wireless Association®	38
Prepared statement	40
Matthew Stein, Chief Technology Officer, Primus Telecommunications Inc.	43
Prepared statement	45
Aaron Foss, Freelance Software Developer, Nomorobo	46
Prepared statement	48

APPENDIX

Response to written questions submitted to Lois Greisman by:	
Hon. Claire McCaskill	61
Hon. Amy Klobuchar	63
Hon. Mark Warner	64
Hon. Dan Coats	66
Response to written questions submitted to Eric J. Bash by:	
Hon. Claire McCaskill	66
Hon. Amy Klobuchar	68
Hon. Mark Warner	68
Hon. Dan Coats	70
Response to written questions submitted to Kevin G. Rupy by:	
Hon. Claire McCaskill	70
Hon. Mark Warner	75
Hon. Dan Coats	77
Response to written questions submitted to Michael F. Altschul by:	
Hon. Claire McCaskill	77
Hon. Mark Warner	77
Hon. Dan Coats	79
Response to written questions submitted to Matthew Stein by:	
Hon. Mark Warner	79
Hon. Dan Coats	82
Response to written questions submitted to Aaron Foss by:	
Hon. Mark Warner	82
Hon. Dan Coats	84

STOPPING FRAUDULENT ROBOCALL SCAMS: CAN MORE BE DONE?

WEDNESDAY, JULY 10, 2013

U.S. SENATE,
SUBCOMMITTEE ON CONSUMER PROTECTION, PRODUCT SAFETY, AND INSURANCE,
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION,
Washington, DC.

The Subcommittee met, pursuant to notice, at 10 a.m. in room SR–253, Russell Senate Office Building, Hon. Claire McCaskill, presiding.

OPENING STATEMENT OF HON. CLAIRE MCCASKILL, U.S. SENATOR FROM MISSOURI

Senator MCCASKILL. Welcome, everyone. This hearing will come to order. We appreciate you being here.

We have all been subject to the frustrations and annoyances of receiving unwanted telemarketing calls, also known as robocalls. It seems these calls always intrude at a very inconvenient time.

Ten years ago, the Federal Trade Commission and the Federal Communications Commission, at the direction of Congress, established a National Do Not Call Registry so that consumers could get some peace and quiet in their homes and stop the torrent of unsolicited telemarketing calls. The idea was simple: voluntarily register your phone number on a centralized list, and telemarketers would be prohibited by law from calling you. The registry has been celebrated across party lines as a successful government program that provides real benefits to consumers.

While the National Do Not Call Registry has been effective at limiting intrusions by legitimate telemarketers, fraudulent robocalls have since filled the void and have become the source of understandable anger and frustration among the public. These automated, prerecorded telemarketing calls that often seek personal information from unsuspecting consumers are an annoyance at best, but they can be devastating for those that are defrauded by them.

It is easy to see how consumers can easily be confused by these calls. One common scam involves a call from Rachel from "Cardholder Services" offering an easy way to reduce consumers' credit card interest rates.

[Audio played.]

Senator MCCASKILL. Another common scam involves robocalls warning consumers that their auto warranty is about to expire.

[Audio played.]

Senator MCCASKILL. In both examples, with the press of a button, the consumer is directed to an individual whose job is to collect financial information in an effort to defraud them. Even pressing the button they claim removes a caller from their list does nothing more than identify a phone number as valid, likely increasing the frequency of unwanted calls in the future.

Law enforcement officials have estimated that telemarketing fraud costs Americans over $40 billion annually. So it is no wonder that robocalls consistently remain a top consumer complaint at the FTC as well as the FCC. The FTC alone receives more than 200,000 complaints about robocalls every month. Complaints received from consumers in the state of Missouri alone have roughly doubled every year since 2009.

The FTC and FCC have taken important steps to try and stop fraudulent robocalls. Both commissions have issued rules restricting robocalls, and they have taken enforcement actions to protect consumers.

Since the National Do Not Call Registry started, the FTC has won more than $250 million in civil penalties and equitable relief for consumers against robocalls. But because these shady companies and individuals are often based overseas and very difficult to locate, the FTC has only been able to collect $15 million out of the $250 million that they have in fact gotten authorization to collect.

Today we will hear from the FTC and the FCC about their efforts to implement the National Do Not Call Registry and other telemarketing rules. We will hear about their successes and their challenges in pursuing fraudulent robocalls, as well as their suggestions for how we can stem the tide of the alarming number of robocalls being placed to Americans every day.

Advances in technology have made it cheap and easy for an individual anywhere in the world with a computer and a broadband connection to make thousands and even millions of robocalls at the push of a button.

Last year, recognizing the limits of regulation and law enforcement in stopping these kinds of calls, the FTC launched a public competition asking American innovators to put forth their best ideas for a technological solution that would weed out fraudulent robocalls. In April, the FTC announced its winners.

Among the three winners of the FTC challenge was Nomorobo, a technology that would screen out fraudulent callers in much the same way that a spam filter screens out unwanted e-mails. We will hear from that product's developer about his innovative idea and what it would take to make it or something like it a viable tool for every American consumer.

It would seem the technological and legal barriers to a technological solution are not insurmountable. Primus, a Canadian telecommunications provider, offers its customers a free "Telemarketing Guard" that similarly screens out fraudulent callers. We will hear from its inventor and chief technology officer about its service.

We will also hear from our domestic wireline and wireless telephone service industries, represented here by the United States Telecom Association and CTIA—The Wireless Association, about the steps the industry has taken, is taking, and could take in the

future to help address the consumer harm from fraudulent robocalls.

Ten years of the National Do Not Call Registry, by all accounts, has accomplished precisely what Congress and the FTC intended. However, fraudulent robocalls and advancing technology has allowed scammers looking to make a quick buck with no regard for the law—they remain a serious annoyance and abuse that faces consumers.

Similarly, the exceptions to the Do Not Call Registry for charities, political calls, and businesses with which consumers have an existing relationship also remain a nuisance for consumers. In exploring regulatory, statutory, or technological changes to address the problem of robocalls, giving the consumers the choice to stop all unwanted calls—charities, political, and businesses with existing relationships to the consumer—stopping all of those calls, regardless of who places them, should be our ultimate goal. The choice here should rest firmly in the hands of the phone that rings.

And I will turn it over now to Senator Heller.

STATEMENT OF HON. DEAN HELLER,
U.S. SENATOR FROM NEVADA

Senator HELLER. Thank you. And good morning. Chairman McCaskill, thanks for holding this hearing.

And I want to thank our witnesses for being here and those in the audience also that are interested in what I think is a very important hearing. And having your participation is important in moving this forward.

Congress has been looking for ways to limit unsolicited telephone calls since 1991 when the Telephone Consumer Protection Act was passed. In 1994, Congress acted again when the Telemarketing Consumer Fraud and Abuse Prevention Act was signed into law. These laws gave the FCC and the FTC commissions the authority to enact regulations on telephone solicitations and the use of automated telephone equipment to make these solicitations.

These laws clearly prohibited any telemarketer from initiating or any seller from causing a telemarketer to initiate an outbound telephone call to a person when that person previously had stated that he or she does not wish to receive a call. So there shouldn't be any confusion as to the intent of Congress when these bills were passed. People have a right to free themselves from telephone solicitations.

As we come up on the 10th year anniversary of the National Do Not Call Registry, I think it is important to note this has been, to a degree, a successful government program. The FTC and the FCC deserve credit for promoting this program and ensuring that it functions correctly.

Solicitors for the most part have honored the wishes of consumers, and when a solicitor has broken the rules, the FTC and/or the FCC have acted appropriately. In fact, on June 27, 2013, the FTC announced a $7.5 million civil penalty for violations by a refinancer of veterans' home loans, which, according to the FTC, is the largest fine that has ever been collected.

Despite the popularity of the Do Not Call Registry and the actions of the FTC and the FCC, there has been a noticeable rise in

the number of illegal robocalls over the last several years. Between October 2008 and September 2009, the FTC received over 700,000 complaints involving calls using a recorded message. Between October 2011 and September 2012, these complaints increased over 2 million.

The FTC and the FCC are actively engaged in stopping these illegal robocalls, but they have admitted to the significant challenges they face against new and emerging technologies, including sophisticated Voice-over-Internet-Protocol enabled auto-dialers and the use of fake caller ID systems.

Companies using auto-dialers can send out thousands of phone calls every minute at almost no cost. Some of these companies do not screen against the Do Not Call Registry and use this solicitation to scam an individual.

I have here with me a recent article in *USA Today* that outlined an example of this type of scam. In fact, it came out this month, on July 4, and it is called "Your Money: Seniors Fight Back Against Robocalls." And it gave a specific example of what is happening out there, and I would like to take a couple of paragraphs, if I may.

> "The automated voice implies that a doctor or a relative signed the consumer up for a medical alert system, and it is all free. Authorities said that, in some cases, after consumers press a button to accept the offer, they quickly receive another call asking for personal information, including credit card numbers. This might be con artists trying to get bank or credit card information or a Social Security number to use in ID theft, or it is a way to pressure seniors into paying for equipment or services that they don't need. The medical alert system scam is in full swing in Michigan, according to the state attorney general's office, as well as in other states, including Pennsylvania, New York, Texas, Wisconsin, and Kentucky."

Today's hearing is an opportunity for the Senate to hear more about the actions of the FCC and the FTC, what they are taking, as well as from the private sector on what technologies are available to help consumers free themselves from unwanted telephone solicitations.

I am looking forward to the testimonies of our panelists and again thank the Chairman for calling this important hearing.

Senator MCCASKILL. Thank you very much.

We will now hear from our witnesses. And we have two witnesses on our first panel. The first panel is Lois Greisman—we are happy to have you here—and Eric Bash, from the FCC and the FTC.

And we are happy to have both of you, and we look forward to your testimony.

Ms. Greisman?

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

Ms. GREISMAN. Thank you. And good morning, Chairman McCaskill, Ranking Member Heller. I am delighted to appear before you this morning to discuss the FTC's work to fight illegal

robocalls. And we are very much appreciative of your leadership in the consumer protection area.

I am also pleased to be sitting next to my friend and former colleague, Eric Bash. Both he and the FCC have been outstanding partners in our fight against telemarketing fraud.

As you noted, by establishing the Do Not Call Registry 10 years ago, the Federal Trade Commission gave consumers an easy-to-use tool to protect their privacy against unwanted calls. I believe, as you indicated, that the do-not-call program has been highly effective in reducing unwanted calls from legitimate telemarketers. Enforcing the do-not-call provisions is a top priority for the agency, and the more than 100 cases filed by the FTC reflect that priority.

But several years ago, we observed a troubling shift in the landscape: robocalls. And I want to talk briefly about what gave rise to the new problem and how we are marshalling all of our resources to tackle illegal robocalls and to protect consumers.

Technological changes in communication services have brought enormous benefits to consumers by way of lower costs and improved services. At the same time, however, fraudsters have also taken advantage of these lower costs, which brought faster and cheaper automated-dialing platforms. Fraudsters have also further exploited caller ID spoofing, which induces the consumer to pick up the phone, while at the same time enabling the scammer to hide its identity and location. And, of course, with phone calls bouncing from country to country all over the world, it is now easier than ever for the robocaller to hide.

With such a cheap and scalable business model, bad actors can blast literally tens of millions of illegal robocalls over the course of a single day at less than 1 cent per minute. These robocalls not only invade consumers' privacy, quite often they pitch goods and services riddled with fraud.

To meet this challenge, we stepped up our law enforcement initiatives. Looking just at the cases we have completed involving robocalls, we have shut down entities that placed billions of such calls and we have obtained court orders totaling more than $200 million in redress or disgorgement and also more than $51 million in civil penalties.

And we have strategically targeted entities that we believe facilitate the illegal robocallers. Specifically, we have sued entities that afford access to massive dialer or voice-blasting platforms that initiate the calls. We have also sued entities known as payment processors that afford access to the financial system and enable the robocallers to process payments from consumers.

And, of course, our coordination with state, Federal, and international partners is as strong as ever. And I am happy to report that some of the individuals sued by the Federal Trade Commission for placing illegal calls have also been prosecuted criminally by the Department of Justice.

We knew, though, that law enforcement was not enough and that more was needed. Toward those ends, we hosted a robocall summit last October, bringing together key players, engineers, academics, industry members, and of course law enforcers. We analyzed the technological changes that had given rise to the robocall tidal wave

and existing structural impediments that served as obstacles to enhanced consumer protection.

Recognizing consumers' frustration with robocalls, which we all share, we wanted solutions now. So we used the summit to launch the FTC's first public contest, which you discussed. It was a huge success in stimulating the marketplace to innovate and develop technological solutions that would help consumers block illegal robocalls.

Mr. Foss's participation in the next panel illustrates the impact of the FTC's challenge to spur competition. He was 1 of 3 winners, but nearly 800 eligible solutions were submitted, many of which presented well-thought-out technical proposals.

And, as always, consumer education and outreach remain indispensable tools that complement our law enforcement and policy work.

Finally, I want to assure you of our ongoing and sustained commitment to protect consumer privacy and halt illegal telemarketing fraud by enforcing the Do Not Call Registry and by tackling illegal robocalls. And I look forward to any questions you may have.

Thank you.

[The prepared statement of Ms. Greisman follows:]

PREPARED STATEMENT OF THE FEDERAL TRADE COMMISSION

Chairman McCaskill, Ranking Member Heller, and members of the Subcommittee, I am Lois Greisman, Associate Director of the Division of Marketing Practices, Bureau of Consumer Protection at the Federal Trade Commission ("Commission" or "FTC").[1] I appreciate the opportunity to appear before you today to discuss the Commission's initiatives to fight illegal robocalls.

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.[2] The Registry, which currently includes more than 221 million telephone numbers,[3] has been tremendously successful in protecting consumers' privacy from the unwanted calls of tens of thousands[4] of legitimate telemarketers who participate in the Registry each year.[5] More recently, changes in technology led to a new source of immense frustration—the blasting of prerecorded messages using Voice over Internet Protocol ("VoIP") technology.[6] In 2008, the Commission responded by amending the TSR to address this problem, prohibiting the vast majority of prerecorded sales calls unless the recipient has provided express written consent to receive them.[7]

---

[1] 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.

[2] 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.

[3] *See* Appendix A, National Do Not Call Registry Active Registrations and Complaint Figures.

[4] For example, in Fiscal Year 2012, more than 28,000 telemarketers accessed the Do Not Call Registry. National Do Not Call Registry Data Book FY 2012 at 8 (Oct. 2012), available at *http://www.ftc.gov/os/2012/10/1210dnc-databook.pdf.*

[5] Humorist Dave Barry called the Do Not Call Registry "the most popular Federal concept since the Elvis stamp." *See* Dave Barry, *Idea for telemarketers: Hang up and go away,* DESERET NEWS, Aug. 31, 2003, available at *http://www.deseretnews.com/article/1006979/Idea-for-telemarketers-Hang-up-and-go-away.html.*

[6] *See* Section II(A), *infra.*

[7] 73 Fed. Reg. 51164 (Aug. 29, 2008); 16 C.F.R. Part 310.4(b)(1)(v). The FTC had already brought robocall-related enforcement actions prior to 2008, alleging that defendants made illegal "abandoned calls," because their robocalls did not "connect the call to a sales representative within two seconds of the completed greeting of the person who answer[ed]." 16 C.F.R. Part 310.4(b)(1)(iv). Any telemarketing campaign consisting solely of prerecorded messages would always violate that provision, and would not meet the abandoned call safe harbor requirements under the TSR. *See* 16 C.F.R. Part 310.4(b)(4). Nonetheless, the Commission amended the TSR to explicitly prohibit unsolicited robocalls, considering it beneficial to make the prohibition more prominent.

Illegal robocalls are still a significant consumer protection problem today, because they repeatedly disturb consumers' privacy and many of them peddle fraudulent goods and services that cause significant economic harm. Therefore, the FTC is using every tool at its disposal to fight them.[8] This testimony describes the Commission's efforts to stop telemarketer violations, including our aggressive law enforcement, initiatives to spur technological solutions, and broad consumer and business outreach.

I. Do Not Call and Robocall Law Enforcement

Since the Do Not Call Registry was established in 2003,[9] the Commission has fought vigorously to protect consumers' privacy from unwanted calls. Indeed, two weeks ago on the 10th anniversary of the Do Not Call Program, the Commission announced that Mortgage Investors Corporation, one of the Nation's leading refinancers of veterans' home loans, will pay $7.5 million, the largest Do Not Call fine the FTC has ever collected.[10] This case is the 105th enforcement action since the Commission began enforcing the Do Not Call provisions of the TSR in 2004.[11] Through these enforcement actions, the Commission has sought civil penalties,[12] restitution for victims of telemarketing scams, and disgorgement of ill-gotten gains from the 298 companies and 234 individuals involved. Although a number of cases remain in litigation, the 81 cases that have concluded thus far have resulted in orders totaling more than $126 million in civil penalties and $741 million in redress or disgorgement. In the first several years of the Registry's existence, consumers reported that the Do Not Call program was highly effective in reducing the number of unwanted telemarketing calls they received.[13]

On September 1, 2009, new TSR provisions went into effect prohibiting the vast majority of sales robocalls,[14] unless the telemarketer has the consumer's prior written authorization to transmit such calls.[15] 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 on robocalls, bringing 34 cases involving illegal prerecorded calls against 97 companies and 77 individuals.[16] These actions have shut down entities responsible for *billions* of illegal robocalls, and the 22 cases that have concluded thus far have resulted in orders totaling more than $51 million in civil penalties and $202

---

[8] *See* FTC Robocall Action Plan, *http://www.ftc.gov/robocalls.*

[9] 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 *http://www.ftc.gov/opa/2003/09/dncok.shtm;* Press Release, Statement of FTC Chairman Timothy J. Muris (Sept. 26, 2003), available at *http://www.ftc.gov/opa/2003/09/dnc030926.shtm.* Congress addressed the first decision in summary fashion by enacting HR 3161 in one day. *See* "HR 3161 (108th) 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 *ttp://www.ftc.gov/opa/2003/09/dnc030926.shtm.* The 10th 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 *http://www.ftc.gov/opa/2004/02/dncappeal.shtm.*

[10] *See* Press Release, Mortgage Broker Targeting U.S. Servicemembers Will Pay Record $7.5 Million to Settle Alleged Telemarketing Violations (June 27, 2013), available at *http://www.ftc.gov/opa/2013/06/donotcall.shtm.*

[11] The 105 Do Not Call actions include cases that involve the rule provisions prohibiting unauthorized robocalls, which also invade consumers' privacy and may be deceptive as well.

[12] As is true of for 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).

[13] For example, in October 2007, an independent study by Harris Interactive® found that of the 72 percent of Americans who had registered their telephone numbers for the Do Not Call Registry, 18 percent reported that they currently received no telemarketing calls, 59 percent reported that they still received some, but far fewer than before they signed onto the Registry, and 14 percent said they received some, but a little less than before they registered. Previous surveys had similar results. *See* Annual Report to Congress for FY 2007 Pursuant to the Do-Not-Call Implementation Act on Implementation of the National Do Not Call Registry, at 4–5, n.10 (July 2008), available at *http://www.ftc.gov/os/2008/07/P034305FY0dncreport.pdf.*

[14] 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 pure political, informational, or survey calls. *See generally* "Complying with the Telemarketing Sales Rule" (Feb. 2011), available at *http://business.ftc.gov/documents/bus27-complying-telemarketing-sales-rule.*

[15] 16 C.F.R. Part 310.4(b)(1)(v). 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).

[16] The FTC filed 12 of the 34 cases before the rule change went into effect on September 1, 2009.

million in redress or disgorgement. Some of the Commission's early robocall cases were against companies with household names such as Dish Network, DIRECTV, and Talbots.[17]

Yet increasingly, robocalls that plague consumers are initiated by fraudsters, who often hide out in other countries in an attempt to escape detection and punishment. One example is the defendants in *FTC* v. *Navestad,* who the Commission successfully traced and sued 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 robocalls, and ordered them to pay $30 million in civil penalties and give up more than $1.1 million in ill-gotten gains.[18] Unfortunately, the two defendants are currently in hiding overseas.

A. Coordination with Law Enforcement Partners

1. State, Federal, and International Coordination

As the law enforcement challenges associated with illegal telemarketing have increased, the FTC's relationships with other agencies have become ever more 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 different forms, including sharing information and targets, assisting with investigations, and working together on long-term policy initiatives. The agency also coordinates with various partners to bring law enforcement "sweeps"—multiple simultaneous law enforcement actions—that focus on specific types of telemarketing fraud.[19] One recent example is a concerted attack on illegal robocalls purporting to be from "Rachel" or others from "Cardholder Services," which pitch a supposedly easy way to save money by reducing consumers' credit card interest rates. 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 same sweep.[20]

2. 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 themselves facing criminal charges and prison time. One example is the *Voice Touch* case, which involved the use of robocalls to advertise an auto warranty scam. The FTC case shut down the scam and resulted in al-

---

[17] *See U.S.* v. *The Talbots, Inc.,* No. 10–cv–10698 (D. Mass. Apr. 27, 2010), available at *http://www.ftc.gov/opa/2010/04/talbots.shtm; U.S.* v. *Dish Network, LLC,* No. 3:09–cv–03073 (C.D. Ill. Feb. 4, 2010), available at *http://www.ftc.gov/opa/2009/03/echostar.shtm; U.S.* v. *DIRECTV, Inc.,* No. 09–02605 (C.D. Cal. Apr. 23, 2009), available at *http://www.ftc.gov/opa/2009/04/directv.shtm.*

[18] *FTC* v. *Navestad,* No. 09–CV–6329 (W.D.N.Y. Mar. 23, 2012), available at *http://www.ftc.gov/opa/2012/04/cashgrant.shtm.*

[19] 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 *http://www.ftc.gov/opa/2012/11/robocalls.shtm;* Press Release, FTC Settlements Put Debt Relief Operations Out of Business (May 26, 2011), available at *http://www.ftc.gov/opa/2011/05/amsdynamic.shtm;* Press Release, FTC Sues to Stop Robocalls with Deceptive Credit Card Interest-Rate Reduction Claims (Dec. 8, 2009), available at *http://www.ftc.gov/opa/2009/12/robocall.shtm;* Press Release, FTC Cracks Down on Scammers Trying to Take Advantage of the Economic Downturn (July 1, 2009), available at *http://www.ftc.gov/opa/2009/07/shortchange.shtm;* Press Release, FTC Announces "Operation Tele-PHONEY," Agency's Largest Telemarketing Sweep (May 20, 2008), available at *http://www.ftc.gov/opa/2008/05/telephoney.shtm.*

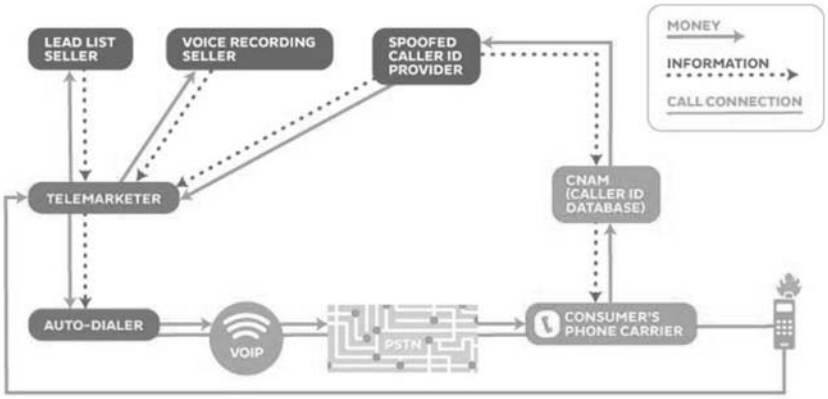
[20] *See* Press Release, FTC Leads Joint Law Enforcement Effort Against Companies that Allegedly Made Deceptive "Cardholder Services" Robocalls (Nov. 1, 2012), available at *http://www.ftc.gov/opa/2012/11/robocalls.shtm.*

most $3.2 million in redress to consumers,[21] and 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 each sentenced to five years.[22]

Another example is Kara Singleton Adams, the leader of a scam that used robocalls to sell worthless credit card interest rate reduction services. Not only did the Commission act to shut down the operation,[23] a Federal jury in Atlanta subsequently convicted Adams on charges of wire fraud and conspiracy, among other things. In 2012, the court sentenced her to more than 17 years' imprisonment. Three of her associates in the scheme also went to prison.[24]

B. Strategic Targeting for Maximum Impact

The Commission constantly seeks innovative ways to maximize its resources and its impact on those responsible for illegal robocalls.[25] Often, telemarketers' deceptive and abusive practices are facilitated by third parties, such as auto-dialers, which provide the software needed to blast out millions of calls, and payment processors, which enable fraudulent telemarketers to reach into consumers' bank accounts. The FTC has increasingly targeted gatekeepers that have tended to service large numbers of rogue telemarketers and therefore offer a way to strike a blow to many lawbreakers with only one case.



Money flows in many directions within a robocall operation. [26]

---

[21] Press Release, FTC Returns Almost $3.2 Million to Auto Warranty Robocall Victims (Aug. 31, 2011), available at *http://www.ftc.gov/opa/2011/08/voicetouch.shtm; FTC* v. *Voice Touch, Inc.,* No. 09CV2929 (N.D. Ill. Aug. 23, 2010), available at *http://www.ftc.gov/os/caselist/0823263.*

[22] Department of Justice ("DOJ") Press Release, "Auto Warranty" Telemarketer Pleads Guilty (June 15, 2012), available at *http://www.justice.gov/usao/ils/News/2012/Jun/06152012_Dolan%20Press%20Release.html;* DOJ Press Release, Update on Transcontinental Warranty Case (Oct. 31, 2011), available at *http://www.justice.gov/usao/ils/Programs/VWA/transcontinental.html.*

[23] *FTC* v. *Econ. Relief Techs., LLC,* No. 09–CV–3347 (N.D. Ga. July 22, 2010), available at *http://www.ftc.gov/os/caselist/0923118.*

[24] 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/usao/gan/press/2012/02-09-12.html.*

[25] As an example, the FTC recently created a robocall "honeypot," which is a group of phone numbers from around the country that the Commission controls, permitting it to receive robocalls directly. This allows the Staff to quickly amass information about who is making the calls and to have recordings in-house, thus facilitating a more rapid law enforcement response.

[26] 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.).

First, the Commission aggressively pursues companies that provide the equipment and software necessary to send out millions of calls, sometimes referred to as "voice broadcasters" or "autodialers."[27] One example is *FTC* v. *Asia Pacific Telecom, Inc.,* in which the FTC alleged that defendants were responsible for violating the TSR by placing billions of prerecorded phone calls on behalf of unscrupulous telemarketers. These robocalls pitched worthless extended auto warranties and credit card interest rate reduction programs while using spoofed Caller ID names—such as "SALES DEPT"—and phone numbers registered to companies with overseas offices in the Northern Mariana Islands, Hong Kong, and the Netherlands. In 2012, the Commission reached a settlement under which the defendants are banned from all telemarketing, from misrepresenting any good or service, and from selling or otherwise benefitting from customers' personal information. The order imposed a $5.3 million judgment that was suspended, based on the defendants' inability to pay, after they had surrendered assets valued at approximately $3 million.[28]

Second, the FTC has increasingly taken action against payment processors when they assist and facilitate telemarketers engaged in deceptive practices, providing access to the financial system and, in turn, consumers' money.[29] Two amended complaints the FTC filed in June provide examples of the agency's enforcement in this area. In both cases, the Commission sued telemarketing operations allegedly peddling bogus credit card interest rate reduction services. After obtaining temporary restraining orders against the defendants and beginning discovery, the FTC moved to amend both complaints to include the defendants' payment processors. The Commission alleges that the payment processors knew, or consciously avoided knowing, key facts about the illegal telemarketing,[30] and chose to continue profiting from the illegal activity by processing consumers' payments to the original defendants.[31]

In sum, the Commission seeks to identify and attack chokepoints for illegal telemarketing.

II. Policy and Market Stimulation Initiatives

Despite the 2008 prohibition of unauthorized robocalls and the Commission's vigorous enforcement efforts, technological advances have permitted law-breakers to continue to profit from illegal robocall campaigns. In the fourth quarter of 2009, the FTC received about 63,000 complaints about illegal robocalls each month.[32] That number ballooned in three years, to an average of approximately 200,000 complaints per month in the fourth quarter of 2012.[33]

---

[27] *U.S.* v. *Skyy Consulting, Inc., also d/b/a CallFire,* No. 13–CV–2136 (N.D. Cal. May 14, 2013), available at *http://www.ftc.gov/os/caselist/1223011; FTC* v. *Asia Pac. Telecom, Inc.,* No. 1:10–3168 (N.D. Ill. Mar. 28, 2012), available at *http://www.ftc.gov/os/caselist/1023060; U.S.* v. *Brian Ebersole,* No. 3:12-cv-00105 (D. Nev. Feb. 29, 2012), available at *http://ftc.gov/os/caselist/0923174; U.S.* v. *Sonkei Commc'ns,* No. SACV11–1777 (C.D. Cal. Nov. 22, 2011), available at *http://ftc.gov/os/caselist/1123060; U.S.* v. *Voice-Mail Broad. Corp.,* No. cv-08–00521 (C.D. Cal. Jan. 29, 2008), available at *http://www.ftc.gov/os/caselist/0523182; U.S.* v. *The Broadcast Team, Inc.,* No. 6:05–cv–01920 (M.D. Fla. Feb. 2, 2007), available at *http://www.ftc.gov/os/caselist/0523025/0523025.shtm.*

[28] *FTC* v. *Asia Pac. Telecom, Inc.,* No. 1:10–3168 (N.D. Ill. Mar. 28, 2012), available at *http://www.ftc.gov/os/caselist/1023060.* The full judgment will become due immediately if the defendants are found to have misrepresented their financial condition.

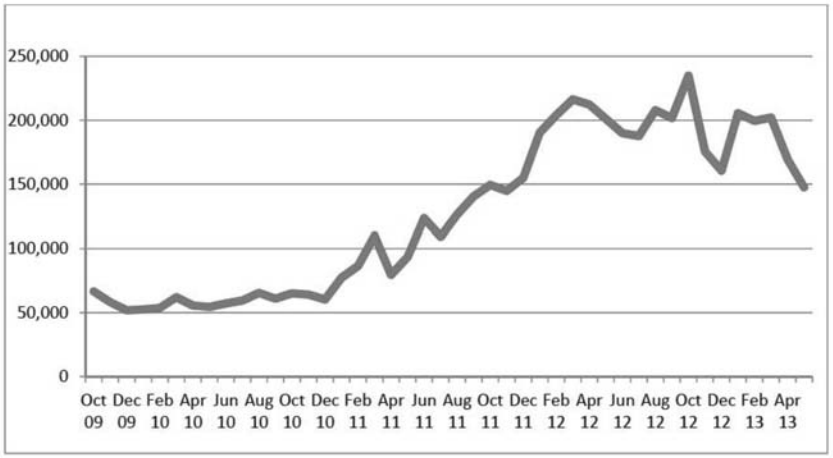
[29] *See, e.g., FTC* v. *Automated Elec. Checking, Inc.,* No. 3:13–cv–00056 (D. Nev. Mar. 13, 2013), available at *http://ftc.gov/os/caselist/1223102; FTC* v. *Landmark Clearing, Inc.,* No. 4:11–cv–00826 (E.D. Tex. June 27, 2013), available at *http://www.ftc.gov/os/caselist/1123117.*

[30] 16 C.F.R. Part 310.3(b).

[31] *FTC* v. *Innovative Wealth Builders, Inc.,* No. 13–cv–00123 (M.D. Fla. June 5, 2013), available at *http://www.ftc.gov/os/caselist/1223127; FTC* v. *WV Universal Mgmt., LLC,* No. 6:12–CV–1618 (M.D. Fla. June 21, 2013), available at *http://www.ftc.gov/os/caselist/1223190.*

[32] National Do Not Call Registry Data Book FY 2010 at 5 (Nov. 2010), available at *http://www.ftc.gov/os/2010/12/101206dncdatabook.pdf.* Since that time, the FTC began separately tracking Do Not Call complaints and robocall complaints based on information provided by the consumer.

[33] National Do Not Call Registry Data Book FY 2012 at 5 (Oct. 2012), available at *http://www.ftc.gov/os/2012/10/1210dnc-databook.pdf.*



Number of robocall complaints filed with the FTC each month [34]

The public's anger has increased with the number of illegal robocalls.[35] Robocalls propagate harmful frauds; indeed, the estimated consumer harm associated with the 22 FTC lawsuits against robocallers that have concluded thus far amounts to more than $202 million.[36] Illegal robocalls also have a significant impact on quality of life by repeatedly invading the privacy and peace of consumers' homes.[37]

A. Coordinating with Technical Experts, Industry, and Other Stakeholders

Convinced that law enforcement alone 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 international government bodies. To that end, on October 18, 2012, the Commission hosted a public summit on robocalls to explore these issues (the "Robocall Summit").[38]

The Robocall Summit made clear that convergence between the legacy telephone system and the Internet has given rise to massive, unlawful robocall campaigns. The telephone network has its origins in a manual switchboard that allowed a human operator to make connections between two known entities.[39] A small group of well-known carriers were in control and were highly regulated.[40] Placing calls took significant time and money, and callers could not easily conceal their identities.[41]

Now, communications technology is universal and standardized such that entrepreneurs can build up a viable telephone services business wherever they find an

---

[34] While this chart suggests recent positive trending of self-reported complaints, it has in no way diminished the Commission's law enforcement efforts.

[35] *See generally* FTC Workshop, *Robocalls: All the Rage* (Oct. 18, 2012). A webcast of the workshop, a transcript of the event, PowerPoint presentations, and other related materials are available at *http://www.ftc.gov/bcp/workshops/robocalls.* References to the workshop transcript ("Tr.") identify the speaker and the transcript page. *See, e.g.,* Zoeller, Tr. at 86–87; Bash, Tr. at 88–89; Maxson, Tr. at 89–90.

[36] This estimate is based on the FTC's equitable monetary relief awards, and excludes civil penalties ordered in the same cases. In addition, it only includes cases that involved robocalls. The estimated consumer harm associated with the FTC's 81 concluded Do Not Call actions amounts to more than $741 million.

[37] *See, e.g.,* Maxson, Tr. at 90–92; Zoeller, Tr. at 86–88; *see also* FTC, *Robocall Challenge Comments* [hereinafter *Public Comment*], available at *http://www.ftc.gov/os/comments/robocallchallenge;* Michelle Block, *Public Comment,* cmt. #565017–00015, at 1 (explaining how robocalls can cause her to lose desired assignments as a substitute teacher).

[38] *See generally* FTC Workshop, *Robocalls: All the Rage* (Oct. 18, 2012), *http://www.ftc.gov/bcp/workshops/robocalls.*

[39] Bellovin, Tr. at 12.

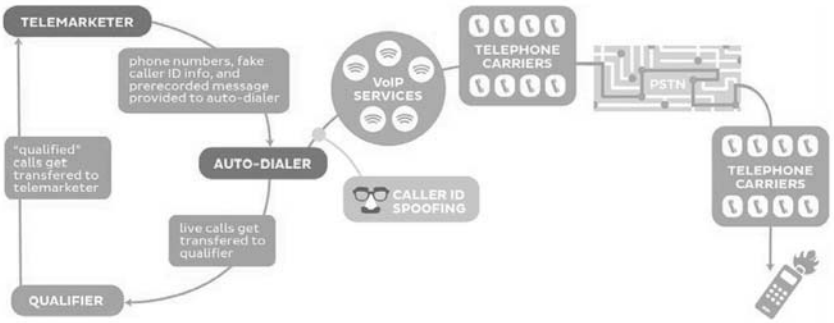
[40] Schulzrinne, Tr. at 22; Rupy, Tr. at 46–47; Diggs, Tr. at 55.

[41] Bellovin, Tr. at 12–17.

Internet connection.[42] As a result, the number of service providers has grown exponentially and now includes thousands of small companies all over the world.[43] In addition, VoIP technology allows consumers to enjoy high-quality phone calls with people on the other side of the planet for an affordable price.[44] 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.[45] 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.[46] Now, robocallers benefit from automated dialing technology, inexpensive long distance calling rates, and the ability to move internationally and employ cheap labor.[47] The only necessary equipment is a computer connected to the Internet.[48] The result is that law-breaking telemarketers can place robocalls for less than one cent per minute.[49] 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, selling the products, or doing all of the above.[50] Because of the dramatic decrease in upfront capital investment and overall cost, robocallers—like e-mail spammers—can make a profit even if their success rate is very low.[51]



Technology enables a cheap and scalable model for robocalls.

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 different VoIP and legacy carriers before reaching the end user.[52] 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.[53] Such a path makes it cumbersome to trace back to a call's inception.[54] 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.[55]

---

[42] Herrman, Tr. at 60–61; Maxson, Tr. at 96.
[43] Schulzrinne, Tr. at 22.
[44] *See, e.g.,* Bellovin, Tr. at 16–17.
[45] *Id.* at 17.
[46] Herrmann, Tr. at 58–59; Schulzrinne, Tr. at 24.
[47] Schulzrinne, Tr. at 24.
[48] Herrmann, Tr. at 59–61.
[49] *See* Dan Weber, Alan Basinger, Dean Willis, and David Schwartz, *Public Comment,* cmt #565017–00014, at 3.
[50] Schulzrinne, Tr. at 20–21; Maxson, Tr. at 95–98.
[51] Schulzrinne, Tr. at 21; Bellovin, Tr. at 16–17.
[52] Panagia, Tr. at 130–32; Bellovin, Tr. at 17.
[53] Panagia, Tr. at. 132; Maxson, Tr. at 100.
[54] Schulzrinne, Tr. at 24–25; Maxson, Tr. at 100; Bash, Tr. at 104.
[55] Panagia, Tr. at 160–61; *see also id.* at 132–133; Schulzrinne, Tr. at 21.

Second, new technologies allow callers to manipulate the caller ID information that appears with an incoming phone call.[56] This "caller ID spoofing" has beneficial uses; legitimate companies adjust their caller ID information regularly so that customers will see the most useful corporate number or name, rather than the phone number from which an agent actually placed the call.[57] However, the same functionality 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.[58] In addition, robocallers can change their phone numbers frequently in an attempt to avoid detection.[59] It is generally illegal to transmit misleading or inaccurate caller identification information with the intent to defraud, cause harm, or wrongfully obtain anything of value, but many robocallers flagrantly violate this law.[60]

Finally, new technologies help robocallers operate outside the jurisdiction where they are most likely to face prosecution.[61] 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 entire globe.

B. Need to Stimulate Technological Solutions

The Commission recognized the need to spur the marketplace into developing technical solutions that could help American consumers block illegal robocalls. Thus, at the conclusion of the Robocall Summit, the FTC announced its first public contest, a "Robocall Challenge" hosted on the challenge.gov platform, with a $50,000 prize for the individual or small team that could propose a technological solution to help consumers block robocalls on their landlines and mobile phones. The Commission also offered a separate award for the best solution by an organization with ten or more employees, which did not have a cash prize.[62]

---

[56] Schulzrinne, Tr. at 24–26.
[57] *See, e.g.,* Panagia, Tr. at 129.
[58] Schulzrinne, Tr. at 21–22.
[59] *Id.* at 24–26; Maxson, Tr. at 97; Bash, Tr. at 103.
[60] *See* 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.).
[61] Schulzrinne, Tr. at 21; Bellovin, Tr. at 16–17.
[62] The judges for the Challenge were FTC Chief Technologist Steve Bellovin, FCC Chief Technology Officer Henning Schulzrinne, and co-Executive Editor of *All Things Digital* Kara Swisher. The basic judging criteria were: Does it work? (50 percent); Is it easy to use? (25 percent);

Continued

The FTC received an astounding 798 eligible submissions, many of which were extremely well-considered technical proposals that moved the ball forward. As a result of the Robocall Challenge, a wide array of people with the necessary technical expertise spent countless hours thinking about these issues. All of the winning proposals were submitted by people who had never previously worked on the specific problem of illegal robocalls. In addition, the Robocall Challenge received an overwhelming amount of public attention and interest, helping the FTC spread the word about illegal robocalls and what consumers can do to fight them.

The primary goal of the Robocall Challenge was encouraging development of realistic ideas for decreasing the prevalence of telemarketing robocalls in a way that the FTC's traditional law enforcement efforts could not achieve alone. On April 2, 2013, the agency announced three winning solutions, which all contained promising ideas about how to address difficult realities such as the limitations of the telecommunications infrastructure and the prevalence of caller ID spoofing.[63] As the winning contestants and others further develop their ideas for introduction into the marketplace, we expect positive results for American consumers.

III. Consumer Education

Public education is an equally 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 agency's behalf.

The FTC delivers actionable, practical, plain language information on dozens of issues. Indeed, the Commission 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 a recorded sales message—and you haven't given your written permission to get calls from the company on the other end—hang up. Period. Other key self-help messages to 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. 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,[64] blog posts,[65] social media,[66] infographics,[67] videos[68] and audio.[69]

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 specifically describing credit card interest rate reduction scams, auto service contract and warranty fraud, and travel-related schemes.[70] 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 that relays some of the best consumer suggestions about what works today to fight robocalls.[71]

---

and Can it be rolled out? (25 percent). For details, see FTC Robocall Challenge Criteria Details, *http://www.robocall.challenge.gov/details/criteria.*

[63] *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;* Appendix B, Summary of Winning Robocall Challenge Submissions.

[64] *See, e.g.,* FTC Robocall Microsite, *http://www.consumer.ftc.gov/features/feature-0025-robocalls.*

[65] *See, e.g.,* FTC Consumer Information Blog, *http://www.consumer.ftc.gov/blog.*

[66] *See, e.g.,* FTC Robocalls Facebook Q&A Transcript (July 17, 2012), *http://www.ftc.gov/opa/socialmedia/facebookchats/1207ftcrobocallsfb.pdf.*

[67] *See, e.g.,* FTC Robocalls Infographic, *http://www.ftc.gov/bcp/edu/microsites/robocalls/infographic.shtm.*

[68] *See, e.g.,* FTC Video and Media, *http://www.consumer.ftc.gov/media.*

[69] *See, e.g.,* FTC Consumer Information Audio, "Hang Up on Robocalls," *http://www.consumer.ftc.gov/media/audio-0045-hang-robocalls.*

[70] *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;* FTC Robocall Microsite in Spanish, "Llamadas automáticas pregrabadas o robocalls," *http://www.consumidor.ftc.gov/destacado/destacado-s0025-llamadas-automaticas-pre-grabadas-o-robocalls.*

[71] Robocall Challenge: Consumer Tips & Tricks (Apr. 2, 2013), *http://www.consumer.ftc.gov/media/video-0086-robocall-challenge-consumer-tips-tricks.*

The Robocall Challenge expanded the reach of the Commission's consumer education messages about robocalls by spurring tremendous media interest. The announcement of the Challenge in October 2012 prompted a nationwide flurry of articles and television stories.[72] When the agency announced the winners in April 2013, it again made headlines in national news outlets and technology publications, also reaching a television audience of an estimated 2.2 million viewers in the first 24 hours following the announcement.[73] Stories explained the problem of illegal robocalls and the FTC's determination to block them from landlines and mobile phones nationwide.

IV. Next Steps and Conclusion

The 10-year old 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 but not limited to 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 block illegal robocalls.
  - We will continue to encourage industry-wide coordination to create and deploy VoIP standards that incorporate robust authentication capabilities.[74] Such 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.

---

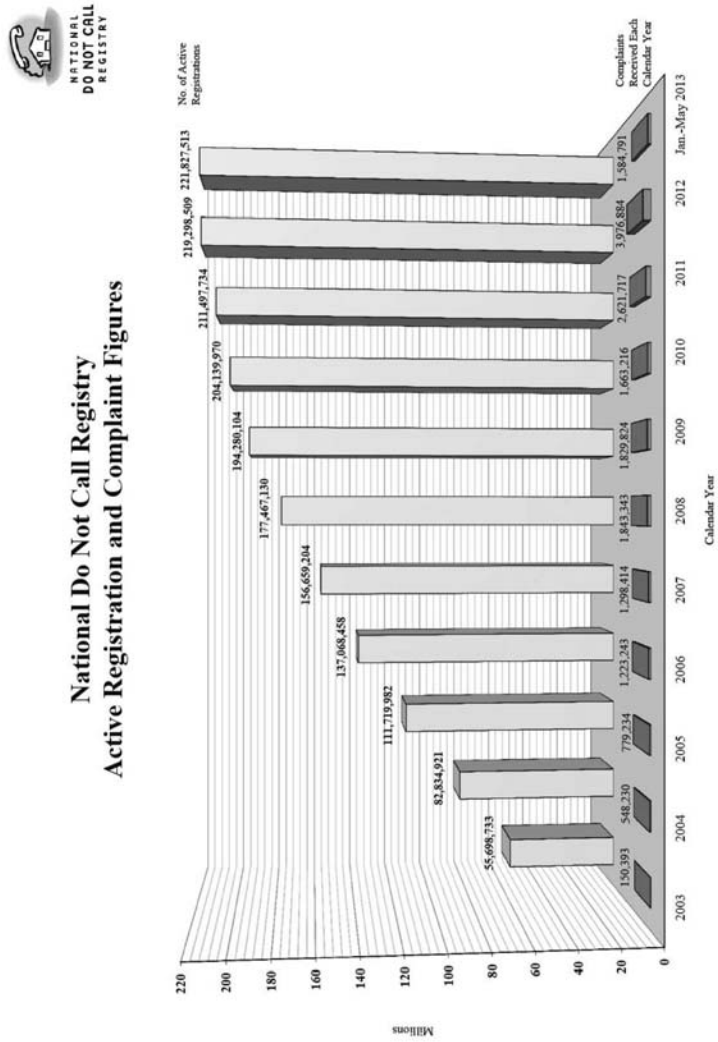
[72] *See, e.g.,* Craig Timberg, *Find a way to block "robo-calls" and win $50K from the FTC,* WASH. POST, Oct. 18, 2012, available at *http://www.washingtonpost.com/business/economy/find-a-way-to-block-robocalls-and-win-50k-from-the-ftc/2012/10/18/a2d648c6-1943-11e2-aa6f-3b636fecb829_story.html;* Trevor Mogg, *Wanna be a national hero? FTC contest offers $50,000 prize for solution to end annoying robocalls,* DIGITAL TRENDS, Aug. 18, 2012, available at *http://www.digitaltrends.com/cool-tech/ftc-contest-offers-50000-prize-for-solution-to-end-annoying-robocalls;* NBC Bay Area, *FTC Holding Anti-Robo Call Contest,* Oct. 20, 2012, available at *http://www.nbcbayarea.com/news/local/FTC-Holding-Anti-Robo-Call-Contest-175078991.html.*

[73] *See, e.g.,* Edward Wyatt, *2 Deterrents to Robocalls Win Contest by FTC,* N.Y. TIMES, Apr. 2, 2013, available at *http://www.nytimes.com/2013/04/03/technology/two-deterrents-to-robocalls-win-ftc-contest.html;* Jon Brodkin, *No more robocalls: New tech automatically hangs up on robots,* ARS TECHNICA, Apr. 2, 2013, available at *http://arstechnica.com/information-technology/2013/04/no-more-robocalls-new-tech-automatically-hangs-up-on-robots;* Cristin Dorgelo, "Innovative Solutions to Fight Illegal Robocalls," Apr. 17, 2013, *http://www.whitehouse.gov/blog/2013/04/17/innovative-solutions-fight-illegal-robocalls.*

[74] This process will require active planning and cooperation in the coming months and years, as we move away from the legacy telecommunications infrastructure and toward a VoIP-based system. Experts around the world, including those involved in the Internet Engineering Task Force ("IETF"), have already begun to explore the technical changes necessary to permit authentication of VoIP calls. In fact, the IETF is in the process of creating a working group about this very topic called "STIR"—Secure Telephone Identity Revisited. Participants in the FTC Robocall Summit also mentioned the Alliance for Telecommunications Industry Solutions as the type of standard-setting group that might assist in organizing the necessary collaboration. Schulzrinne, Tr. at 167*; see also* Rupy, Tr. at 51, 67; Diggs, Tr. at 68–69; Whitt, Tr. at 208–09; *see generally* Paula Bailey-Stine, *Public Comment,* cmt #565017–00022, at 3–5.

APPENDIX A

National Do Not Call Registry Active Registrations and Complaint Figures



APPENDIX B

Summary of Winning Robocall Challenge Submissions

FTC Robocall Challenge Winners
April 2, 2013

BEST OVERALL SOLUTION AWARD (Tie, winners receive $25,000 each):

Serdar Danis

Serdar Danis is a computer engineer who, in his free time, enjoys entering crowd-sourced technology contests such as patent research contests through Article One Partners and innovation contests through InnoCentive. This was his first time entering a contest through ChallengePost. Mr. Danis has several patent applications pending pertaining to this solution and also other inventions. You can direct inquiries about his solution to robocallchallengewinner@gmail.com.

For his solution, *Robocall Filtering System and Device with Autonomous Blacklisting, Whitelisting, GrayListing and Caller ID Spoof Detection*

This solution involves a software application that can authenticate caller ID information as either authentic or spoofed, and display this information to the customer. It can be implemented through a customer-installed software application on smartphones and certain telephone systems, through updates to smartphone operating systems or carriers' software, or through a hardware device at the customer premises. In addition to authenticating caller ID information, the system depends on white and black lists that can be populated manually or autonomously and then aggregated into global white and black lists. Calls with authentic caller IDs on private or global white lists can be put through to the customer and calls from spoofed caller IDs or authentic callers IDs on the private or global black lists can be dropped. Any number not on a white or black list, or not authenticated, can be handled based on customer preferences, such as forwarded to voice mail or subjected to human verification without ringing the customer phone. Human verification would rely on continuously changing pre-recorded questions presented to the caller, which would be difficult for a computer to answer. The solution stops those who abuse the telephone system without inconveniencing regular callers.

Aaron Foss

Aaron Foss is a freelance software developer based in Long Island, New York. He went through the TechStars NYC program (Summer 2011) and is co-founder and lead developer of SmartChemo. You can direct inquiries about his solution to aaron@nomorobo.com or 631-406-9283.

For his solution, *Nomorobo*

Nomorobo uses an existing feature of the current phone system along with the power of cloud computing to fight back against illegal robocallers. By using simultaneous ringing – which is widely available through most phone carriers - the call is split and routed to the Nomorobo server as well as the user's phone. Instantly, Nomorobo analyzes the call and determines the threat level by using machine learning to identify and adapt to new robocallers based on their calling patterns. Nomorobo inspects the CallerID header, analyzes the frequency of every call, and compares this data to its real-time black and white lists. Potential robocallers are presented with an audio CAPTCHA for final verification while legal robocallers have their phone numbers whitelisted to guarantee message delivery. If it's an unknown robocall, Nomorobo answers and immediately hangs up. If no threat is detected, Nomorobo does nothing and the call goes through like normal. All of this happens instantly, before the consumer's phone begins to ring. Nomorobo works with any kind of phone, no additional hardware is necessary, and no infrastructure changes are required by phone companies.

APPENDIX B (Con't)

TECHNOLOGY ACHIEVEMENT AWARD (Non-monetary):

Daniel Klein and Dean Jackson, from Google

Mr. Klein and Mr. Jackson are engineers based out of the Google office in Pittsburgh, Pennsylvania. You can direct inquiries about their solution to Google's press office.

For their solution, ***Crowd-Sourced Call Identification and Suppression***

Google's robocall concept could give consumers the power to block robocalls -- and to allow that information to be used to shield all consumers from robocallers even before their phones ring. The concept could work across all phone platforms as deployed via a smartphone app, changes to VoIP telephone software, or hardware devices. In each case, consumers could easily indicate whether an unknown number should be blocked in the future, which could then be communicated to a centralized database. After a number of people marked a caller as needing to be blocked, that caller could be blocked for everyone else that chose to use the system. The system would include a specialized mechanism to combat CallerID spoofing. In addition, before adding a number to the centralized database, many factors could be considered such as call volume, frequency, and inbound/outbound ratio. These factors could be computed dynamically, adjusting the behavior of the system to match current calling patterns. Also, the system could use a whitelist to keep some numbers out of the database. By using aggregated data about the incoming phone numbers in this manner, this concept could quickly identify and block robocallers and the fraudsters that use these automated calls to swindle consumers.

Senator MCCASKILL. Thank you very much, Ms. Greisman. Sorry I mispronounced your name at the beginning.

Mr. Bash?

STATEMENT OF ERIC J. BASH, ASSOCIATE CHIEF, ENFORCEMENT BUREAU, FEDERAL COMMUNICATIONS COMMISSION

Mr. BASH. Good morning, Chairman McCaskill and Ranking Member Heller. I am Eric Bash, Associate Chief of the Federal Communications Commission's Enforcement Bureau. Thank you for the opportunity to appear before you today.

Almost every American has personal experience with robocalls, and almost everyone is fed up with them. With our own six-figure volume of complaints last year, we hear you.

So what exactly is a robocall at the FCC? What makes one illegal under our rules? What are we doing about them? And how could enforcement be enhanced?

At the FCC, we use the term "robocalls" to refer not to just prerecorded calls but also autodialed calls, regardless of whether the call is live or prerecorded. Under FCC rules, these calls cannot be made to a number assigned to emergency telephone lines, lines in guest rooms in health-care facilities, or wireless devices except in two cases: one, for an emergency purpose; or, two, with the prior express consent of the called party. That means that robocalls generally cannot be made to wireless devices or the other restricted lines I mentioned, even for a noncommercial purpose.

Prerecorded calls to residential landlines are subject to fewer limitations, but only a few less. Prerecorded calls to residential lines can be made for non-emergency purposes without the called party's consent, but only if the call is made, one, for a noncommercial purpose or, two, for a commercial but not telemarketing purpose or, three, by certain defined persons to deliver a health-care message or, four, by or for a nonprofit organization. Any otherwise

permissible robocall must also include certain identifying disclosures to be legal.

The FCC also recently adopted rules to create a special do-not-call list for lines answered by public safety answering points and is prohibiting all autodialed calls to numbers registered on that list.

As you know, the FCC shares responsibility at the Federal level with the Federal Trade Commission for enforcement against telemarketing calls, including telemarketing robocalls. The agencies maintain consistency between their rules pursuant to statute and a memorandum of understanding. Both agencies' rules prohibit making prerecorded telemarketing calls to any telephone number, mobile or residential, except with the express prior written consent of the called party.

Congress has empowered the FCC to enforce the Communications Act in several ways. The tool the agency uses most is assessment of a monetary forfeiture. Under the Communications Act, the FCC may not impose such a forfeiture on a non-licensee, meaning someone other than broadcasters or carriers, for example, until it first issues a citation to the wrongdoer for an illegal act and the wrongdoer thereafter repeats the same kind of misconduct. The maximum penalty for non-licensees is generally $16,000 or about one-tenth the amount of that for carrier licensees.

Over the last decade, the FCC has issued more than 500 citations and taken approximately 10 forfeiture-related actions involving millions of dollars of penalties for robocall rule violations.

Our two most recent robocall actions cited operators of platforms that, according to our investigations, made almost 6 million impermissible robocalls to mobile phones in just several months. The operators offered a service to call the phone numbers provided by their clients, to deliver the prerecorded message provided by their clients, and to display on consumers' caller ID the telephone numbers provided by their clients.

By focusing on these operators, rather than their individual clients, we hope to maximize the impact of our existing enforcement resources. Numerous other platform providers remain under investigation.

Significant law enforcement challenges remain, however. A fundamental problem is identifying the wrongdoer. Robocallers often spoof the number from which they are calling, so inquiries to carriers that control the numbers displayed to the consumers may not yield useful identifying information. Investigators must therefore work backward, subpoenaing the called parties' carrier and, in turn, all intermediate carriers to find out where the call originated.

Time is of the essence because some providers do not appear to keep relevant records for much time and because the FCC must initiate any forfeiture proceeding within 1 year of a violation.

There are several ways in which the FCC's enforcement tools might be enhanced. Congress might, for example, consider changing the FCC's authority by, one, allowing the FCC to impose a forfeiture on non-licensee robocaller violators without first issuing a citation; two, expanding the current statute of limitations from 1 year to 2; and, three, increasing the maximum forfeiture that the FCC can impose on non-licensee robocallers.

To address the spoofing that complicates law enforcement, Congress might also consider extending the scope of the prohibition in the Truth in Caller ID Act against changing caller ID for harmful purposes to apply to offshore callers and more VOIP providers than just those who originate and terminate traffic on the public switched telephone network. Congress might also consider giving the FCC regulatory authority over third-party spoofing providers.

There are also technological ideas on the table that may afford additional consumer protections from illegal robocalls. The FTC-sponsored contest helped to identify some of these ideas, and an industry standards organization is working with FCC technical staff on still more ideas.

Thank you for the opportunity to appear before you today, and I welcome any questions you may have.

[The prepared statement of Mr. Bash follows:]

PREPARED STATEMENT OF ERIC J. BASH, ASSOCIATE CHIEF, ENFORCEMENT BUREAU, FEDERAL COMMUNICATIONS COMMISSION

Good morning Chairman McCaskill, Ranking Member Heller, and Members of the Subcommittee. My name is Eric Bash, and I am an Associate Chief in the Enforcement Bureau of the Federal Communications Commission (FCC.) My responsibilities include oversight of the agency's enforcement of provisions in the Communications Act and the FCC's rules that are designed to protect consumers of telecommunications services. These provisions and rules include restrictions against "robocalls," which is a popular shorthand way for to calls made using a prerecorded message or using an autodialer, whether the message is live or recorded. Thank you for the opportunity to appear today to address the FCC's role in combatting these calls.

Almost every American is familiar with robocalls from their own personal experience. Who, for example, hasn't answered a phone call at one time or another, only to hear a recorded message encouraging the called party to "press 1" to claim a free vacation? Or to redeem a "last chance" to lower mortgage rates? Or to extend an auto warranty? There are certainly legitimate robocalls—such as those consumers want, for example, to alert them to changes in school schedules—but most of these calls, at best, annoy consumers, and at worst, trick them into fraudulent transactions.

At the FCC, we are also aware of, and take very seriously, the problem of robocallers making huge volumes of calls, either simultaneously or in rapid succession, to multiple lines at the same place of business, in order to overwhelm it. When these robocalls target first responders or hospitals telephone lines, they can threaten to interfere with legitimate calls that, if left unanswered, may literally mean the difference between life and death.

The prevalence of these types of robocalls is on the rise. This is because of the ready availability and low cost of phone service and the software needed to make the calls, as well as the ability of callers to "spoof" the number from which they are calling in an attempt to disguise who they are and avoid detection. It is no surprise, then, that robocalls are an increasing source of consumer complaints in recent years at the FCC, with the number of complaints about the topic doubling in the past two years to over 100,000 filed in 2012. While this is only a fraction of the total number of robocall complaints filed each year at various agencies, the volume at the FCC alone still speaks volumes, so to speak, about the extent of the problem. The FCC is also hearing more and more from first responders who are victims of sporadic autodialing.

I have been asked to address you this morning to explain the FCC's role in combatting illegal robocalls. In doing so, I think it would be helpful first to describe the applicable law that Congress has charged the FCC with enforcing. I will then turn to the enforcement powers and process that Congress has given the FCC to discharge its responsibilities, and highlight some recent actions the agency has taken. I will close my prepared remarks by identifying some enforcement challenges we face in combatting illegal robocalls, and how we might begin to overcome them. I will also explain how the Federal Trade Commission's authority in this area complements the FCC's.

FCC-Enforced Legal Standards

So what makes a robocall illegal under FCC-enforced standards? It depends upon the kind of number called, and the purpose of the call. The FCC's rules in this area flow directly from the Telephone Consumer Protection Act of 1991, or TCPA.

Restricted Lines. Under the FCC's rules, no telephone call can be made using an autodialer or an artificial or prerecorded voice to certain "restricted lines" for non-emergency purposes without the called party's prior express consent. These "restricted lines" are emergency telephone lines (such as 911 lines), lines in guest/patient rooms in health care facilities, and all numbers assigned to mobile devices. Note that this restriction applies not just to calls with an artificial or prerecorded voice, but also to live calls made with an autodialer. For telemarketing calls, the prior express consent will have to be in writing after October 16, 2013.

In this day and age of heavy mobile phone use, it may be worth repeating that the FCC's rules flatly prohibit all autodialed or prerecorded calls to mobile phones made for a non-emergency purpose without the called party's permission. It does not matter whether the call is to persuade the called party to buy some *thing* or to support some *cause.* And, despite common mischaracterizations of the law, it does not matter whether the called party is charged for the call, or whether the content of a message is blasted by text or voice. (The FCC has been clear that "autodialed" text messages fit within the restriction.) What matters is that a robocall was placed to a mobile phone, for a non-emergency purpose without the called party's consent. Robocallers can ensure that they are complying with this restriction by scrubbing their call lists against the telephone numbers that several commercial services offer to identify those assigned to mobile telephones.

Residential Lines. Like calls made to restricted lines, calls using an artificial or prerecorded voice can be lawfully initiated to a residential line for an emergency purpose or with the called party's prior express consent, and, for telemarketing calls, the prior express consent will have to be in writing after October 16, 2013. But calls using an artificial or prerecorded voice can also be lawfully initiated to residential lines under several other circumstances. Such calls may be made if they contain certain disclosures and: (1) the call is made for a non-commercial purpose; or (2) the call is made for a commercial purpose but does not constitute telemarketing; or (3) the call delivers a health care message and is made by certain defined persons; or (4) the call is made by or for a tax-exempt non-profit organization. The disclosures must identify, at the beginning of the call, the person or entity responsible for initiating the call, and, during or after the message, provide a telephone number where that person or entity can be reached. And it is important to note that the restrictions for residential lines apply only to calls using prerecorded messages, not those using an autodialer.

PSAP Lines. Pursuant to legislation passed last year, the FCC has also adopted rules that will create a special do-not-call registry for lines answered by public safety answering points (PSAPs), and has prohibited autodialed calls to numbers registered on that list. The legislation was designed to address the situation of autodialers placing calls to telephone numbers associated with emergency lines, and thereby precluding legitimate emergency-related calls from coming through. Note that this restriction applies to all autodialed calls, whether live or prerecorded.

FCC Enforcement Process

Congress has empowered the FCC to enforce the Communications Act, including the TCPA, and the agency's implementing rules and orders, in several ways. In designating the FCC as the Federal agency that licenses and regulates those involved in electronic communication by wire or radio, Congress created different enforcement mechanisms that vary in terms of availability and severity according to whether the wrongdoer holds (or should hold) a license from the FCC.

For licensees, such as broadcasters and carriers, the FCC's most powerful tool to enforce compliance with the law is to revoke a license for non-compliance, or deny issuance or renewal of the license. Because obtaining or retaining an FCC license may literally mean the difference between economic life and death for a licensee, the FCC does not resort to this remedy except in the most egregious cases of non-compliance.

The FCC more commonly enforces the Communications Act, including the TCPA, and its implementing rules and orders by imposing monetary penalties. To do so, the FCC must either conduct a hearing, or issue a notice of apparent liability for forfeiture, or NAL. For administrative efficiency and other reasons, the agency most frequently follows the latter approach. A party subject to an NAL has an opportunity to submit factual and legal arguments in response explaining why the forfeiture proposed should be canceled or reduced. The FCC evaluates the response, and assuming it concludes that a forfeiture of some amount should be assessed,

issues a final order imposing the penalty. If further legal action is necessary to collect the penalty, the FCC must refer the matter to the U.S. Department of Justice. While the FCC may impose a forfeiture either through a hearing or an NAL against both licensees and non-licensees, the Communications Act distinguishes between these groups, both in terms of process required and the severity of the penalty permitted. For non-licensees, under current law, generally speaking the FCC may impose a maximum penalty of $16,000 per violation, but may do so only after first issuing a citation to the wrongdoer finding that it has engaged in an illegal act, and, subsequent to the citation, the wrongdoer again engages in violations of the same type. By contrast, for carriers, which operate under express authorization from the FCC, the agency may impose a forfeiture of up to $150,000 per violation, without first citing the carrier. Likewise, broadcasters, which operate pursuant to an FCC license, generally speaking are directly subject to forfeitures of $37,500 per violation, without a prior citation. (These forfeiture amounts are those generally applicable for violations of the Communications Act, including violations of TCPA. Note that Congress has adopted other penalty structures in certain other circumstances.)

The Communications Act also authorizes the FCC to issue an order to cease and desist against anyone violating a law it enforces; the Act envisions a trial-type administrative hearing in order to invoke this remedy. The Communications Act also authorizes the Department of Justice to obtain an injunction on behalf of the FCC.

FCC Enforcement Actions

Using these enforcement powers, in the last decade, the FCC has issued more than 500 citations, and taken approximately 10 penalty-related actions involving around $3.5 million, for violations of its robocall rules. (These are in addition to more than 500 citations and approximately 20 penalty-related actions for do-not-call telemarketing violations.) The FCC also issued an Enforcement Advisory last fall, as the election season was in full swing, to remind campaigns and those making calls on their behalf of the rules of the road for making robocalls. It is worth reiterating, as this advisory suggests, that the sweep of our rules is broad; they address not just telemarketing robocalls, but all robocalls, including political robocalls and robocalls to "restricted lines" without the called party's permission.

I want to highlight the FCC Enforcement Bureau's two most recent robocall enforcement actions, taken just a few months ago. These reflect a change in approach designed to enhance the effectiveness and efficiency of agency enforcement in this area. Instead of targeting a single enterprise or individual behind a single type of robocall, the Bureau cited operators of platforms that make prerecorded calls in violation of the robocall rules. These operators offered a service whereby third-party clients could transmit or upload to the operator for delivery to specified called parties, along with the telephone numbers to which the operator was to place the calls. They could also choose the phone number that they wished the platform to display to the called party. The investigations leading to these citations found that the operators had made nearly *six million* impermissible robocalls in *just several months.* By addressing the platforms that make the illegal calls, as opposed to focusing on end-users behind such calls, we expect to cast a wider net and more efficiently use our limited resources to multiply the impact of our enforcement efforts. While I cannot comment on pending law enforcement matters where we have not yet taken a public action, I can say that these platforms remain an area of emphasis. I also want to add that, while the express language of the TCPA disallows "making" prerecorded calls under the circumstances that were the subject of our platform citations, and unambiguously outlaws platforms from "making" calls like those I have described, the FCC recently issued a ruling to re-emphasize that anyone who makes a call on behalf of a third party is liable for violations of FCC rules implementing the TCPA. The third party on whose behalf an illegal call is made may also be vicariously liable for the violation.

Law Enforcement Challenges

Notwithstanding the actions the FCC and others have taken over the last decade, significant challenges remain to stopping illegal robocalls, especially from those attempting to entice the called party to engage in a fraudulent transaction.

Identification of Perpetrator. A fundamental problem for law enforcement in dealing with fraudulent as well as other robocallers remains identifying the parties responsible for them. Consumer complaints filed with the FCC about robocalls ordinarily provide little more information than the names used by callers, and the telephone numbers displayed on the called parties' caller ID, because this is normally all the data available to the complainant. But these pieces of information are not sufficient to enable prompt enforcement action if the robocaller has used a fake and nondescript name, and "spoofs" the number from which it is calling—that is, pre-

sents on the called party's caller ID a number other than the one from which the robocaller is actually calling. In these circumstances, subpoenas issued to the carrier that controls the apparent originating number may not yield identifying information. As a result, investigators must work backward and subpoena the called party's carrier for information about where that carrier obtained the call. Because multiple carriers may be involved in handling a single call, investigators may need to repeat this process a number of times before they can identify the true originator of a given call. Time is of the essence, as carriers maintain this kind of call detail record only for limited periods of time, and because the FCC is required by law to act within a year of a violation if it intends to impose a forfeiture penalty. As a result, the FCC is exploring ways to streamline the subpoena process with carriers.

FCC Enforcement Options. Entities that or individuals who do not hold a Commission authorization and are not required to have one pose particular enforcement challenges. As I have noted, while we may cite a wrongdoer, finding that its conduct violates the law, we may not impose a monetary penalty directly. And while citations may work reasonably well for those who are unknowingly or negligently violating the regulatory and statutory provisions on robocalls, we believe a more immediate and tangible penalty may be needed to cause those who are intentionally violating the law to bring their conduct into compliance. Swift, stern enforcement powers are especially needed against fraudulent robocallers who use different names, change addresses frequently, and appear to open and close businesses on a regular basis. Law enforcement is also complicated, of course, when the robocaller appears to be physically located outside of the United States.

Federal Trade Commission

As Members of this Subcommittee know, the FCC shares enforcement responsibility at the Federal level with the Federal Trade Commission (FTC) for combatting telemarketing calls, including telemarketing robocalls. The agencies maintain consistency between their telemarketing rules pursuant to the Do-Not-Call Implementation Act of 2003. Thus, with respect to robocall rules in particular, both agencies' rules will, as of October 16, 2013, prohibit making prerecorded telemarketing calls, except with the prior express written consent of the called party. This consent is in addition to, and distinct from, registering a phone number on the national do-not-call list.

To coordinate the exercise of their joint responsibilities in the telemarketing area, the FCC and the FTC also entered into a longstanding Memorandum of Understanding. Under the MOU, the agencies have agreed to, among other things, meet at regular intervals to discuss matters of mutual interest, to share complaints regarding potential violations of Federal telemarketing rules, and to work together to implement consistent and non-redundant enforcement of such rules. In fact, Ms. Greisman and I met with our agencies' respective staff just last week for law enforcement coordination purposes.

One particular way the agencies have coordinated enforcement in the telemarketing area is by each agency focusing on the areas where its enforcement tools are best suited to the misconduct at issue. For example, the FCC's authorization over carriers provides a very powerful means of pursuing and remedying violations involving them. (While the FCC has not yet taken any action against a carrier for robocall violations, it has for do-not-call violations.) Moreover, our regulatory expertise with carriers gives us a familiarity with their processes that is uniquely helpful to us in obtaining the information we need to pursue robocall violations. The FTC, on the other hand, possesses particular advantages in discouraging robocall activity in connection with its efforts to thwart the fraudulent activity that often underlies robocalls. The FTC's ability to bring suit against non-licensee miscreants, freeze assets and obtain restraining orders based on fraudulent activity can be quite effective in discouraging robocall behavior, although it is also quite resource intensive.

Overcoming Enforcement Challenges and Further Protecting Consumers

To maximize the FCC's enforcement impact, Congress might consider making certain changes to the FCC's powers. For example, Congress might consider:

- allowing the FCC to impose a forfeiture on non-licensee robocall violators without first having to issue a citation;
- expanding the current statute of limitation from one year to at least two years, given the frequent need to engage in the time-consuming process of identifying callers by working backwards through a chain of carriers; and
- increasing the maximum forfeiture that the FCC can impose on non-licensee robocallers.

Congress might also consider revising the Truth-in-Caller-ID Act of 2010. This statute prohibits spoofing when done by persons in the United States with the intent to defraud or cause harm or wrongfully obtain anything of value. When the FCC adopted implementing rules approximately two years ago, the agency's Chairman sent a report to Congress with proposed additional changes to the statute, including:

- expanding the scope of the prohibition to apply to persons outside of the United States when their spoofing is directed at people inside the United States;
- clarifying whether the existing restrictions should apply to Voice over Internet Protocol providers that enable only outbound calls; and
- giving the FCC appropriate authority to regulate third-party spoofing services.

As the report explained, the Department of Justice has advocated that third-party spoofing providers should be required to verify that a user has authority to use the telephone number it is seeking to have substituted for its own, in order to make it easier to identify actors who use these services for fraudulent or other harmful purposes.

Technological solutions that empower consumers to block illegal robocalls so that they do not receive them in the first instance may also be helpful in thwarting illegal robocalls. An industry standards organization is currently working with FCC technology staff to design a system whereby originating carriers would cryptographically sign calls, so that receiving carriers can validate that callers in fact have the right to use the number they are using; as more carriers implement such solutions, methods could be developed to protect consumers from calls where the number cannot be validated. The staff involved hope that the joint effort may lead to implementable specifications in about a year. Other ideas about technical solutions were presented at the FTC's robocall summit last fall, as well as in the FTC's contest that closed just a few months ago.

As legal changes and technological solutions are being considered, the FCC, along with the FTC and others, must continue to educate consumers about how to protect themselves from illegal robocalls, and when they receive them, how to file the most useful complaint with law enforcement. Such education includes discouraging consumers from interacting with any of the prompts in a robocall, and making sure that their complaints include as much information as possible, including the exact time and date of the call they received, and the carrier to whose service they subscribe. The FCC's website has its own consumer education materials, complaint forms, and cross-references useful material provided by the FTC.

Conclusion

Thank you again for the opportunity to appear before you today to explain the FCC's role in addressing illegal robocalls. I welcome any questions you have for me.

Senator MCCASKILL. Thank you both.

Well, let me start with you, Mr. Bash. Do the statutes that guide your enforcement in this area, do they provide for the possibility of prison?

Mr. BASH. They do not.

Senator MCCASKILL. OK.

And how about anything that you can do on your end at the FTC?

Ms. GREISMAN. We do not have criminal law enforcement authority, but we work regularly with the Department of Justice and criminal authorities at the state level.

Senator MCCASKILL. Is there an applicable statute that you can utilize at the Federal level that provides prison for people who do this?

Ms. GREISMAN. Not on the part of the Federal Trade Commission.

Senator MCCASKILL. Yes. Well, so nobody has gone to jail, right?

Ms. GREISMAN. There have been criminal prosecutions of individuals who have been sued by the Federal Trade Commission for en-

gaging in illegal robocalling in civil cases. The criminal prosecutions, I believe, have focused on allegations of wire fraud.

Senator MCCASKILL. OK. And so the wire fraud prosecutions that have taken place in the area dealing with robocalls, has anybody gone to prison? Do you know?

Ms. GREISMAN. Yes, I believe there have been significant sentences.

Senator MCCASKILL. OK. Well, we need to get that word out. It seems to me that, you know, these guys aren't really afraid of you. I don't think that they are very nervous at all. Because it seems to me that they are just all in at this point.

They have the technology to do massive amounts of calls for literally scraps off the table, with great potential of payoff. I mean, this is a criminal sandbox, and I can't imagine a more fun place to hang out if you are somebody who is a criminal. And I think we need to look at that also.

Would some additional criminal statutes help you, Mr. Bash?

Mr. BASH. I think additional legislation like that could be useful. The FCC, like the FTC, is not a criminal law enforcement agency, so I don't think we would be taking the actions ourselves there. But certainly——

Senator MCCASKILL. I guarantee you that criminal prosecutions in this area would be way more popular than just about anything else the Department of Justice does.

Mr. BASH. I am sure they would be.

Senator MCCASKILL. What about the folks that are processing the payments on this? Do you feel like you have adequate statutes to go after them and put them in prison?

Because somebody is moving this money through electronically, and they are making money off of it. And they have to know that this is not mom and apple pie that is being sold here, that they are making money off of.

I know that we have had some actions against the payment processors. Are these companies that we would recognize that are processing these payments?

Ms. GREISMAN. The Federal Trade Commission has taken action against payment processors for well over 10 years. The most recent ones were brought under the Telemarketing Sales Rule. They are alleged to have assisted and facilitated the illegal robocaller. And we have a burden of proof of showing that there is some level of knowledge there.

I think, you know, there are two scenarios. There are those who facilitate fraud who are completely in cahoots with the fraudster; they know exactly what is going on. And then there are those who either do know or consciously avoid knowing. And, you know, it is just going to turn on the facts.

But it is not necessarily the case that those who facilitate fraud, gatekeepers or chokepoints, are completely in bed with the fraudsters. They maybe avoid knowing what is going on.

Senator MCCASKILL. Well, yes, but they are not hard to catch. Because if you set them up, if they are trying to avoid knowing, 9 times out of 10 if you send somebody in under cover to say the appropriate things, they are going to say something in reply that makes it clear that they are trying to—it is a little bit like the guy

driving the getaway car: "Well, I had no idea he was in there robbing the bank. You can't hold me liable." Well, under criminal law, we can.

Ms. GREISMAN. You are right. And you are absolutely——

Senator MCCASKILL. And this is, they are driving the getaway car.

Ms. GREISMAN. Yes, they are facilitating the illegal——

Senator MCCASKILL. Are these companies that we would recognize that are processing these payments? Are these, you know, the mainstream payment processors that process my payments to iTunes or my payments to Amazon? Are they the same people?

Ms. GREISMAN. I am not sure that any of the ones that the FTC has sued of late are necessarily recognizable names. But we certainly will be looking across the industry to see whether there are any entities who facilitate——

Senator MCCASKILL. That is reassuring that you are looking. And I certainly wasn't trying to make any allegation against those companies, that they are involved in this. I am just, you know—obviously, we are processing a lot of payments electronically these days. And there are recognized, reputable companies, and then there are others. And I am just assuming that this is all in the others" space.

Ms. GREISMAN. We look at each case as we see it——

Senator MCCASKILL. OK.

Ms. GREISMAN.—and we see who is involved.

Senator MCCASKILL. Let me finish up, and then I will give it to Senator Heller.

On the caller ID spoof, I have been asking my family to keep track of calls. And, in fact, I have gotten a few. I have learned something very important. If you ask for a phone number, they hang up. They are all trained that if you ask them for a phone number, they immediately hang up, because they know there is not a good ending there. So they just move on to the next call—if you have somebody live on the other end.

I also have learned from my family members that they are using fraudulent caller ID numbers, that if you are getting a call in Saint Louis or if you are getting a call in Kansas City, the area code that they are using is, in fact, a state area code even though the call is being generated from far away, many times not even in this country.

Can we go after the companies that are providing these numbers that clearly are not the numbers they are calling from?

Mr. BASH. The folks who are providing the false number?

Senator MCCASKILL. Yes.

Mr. BASH. So let me get at that a couple of different ways.

Under the robocall rules, it is really the legal standard is the person who is making the call, who is initiating the call. That is who is responsible under our law for a violation.

There is, as I mentioned, the Truth in Caller ID Act that prohibits spoofing caller information with an intent to defraud or cause harm or wrongfully obtain anything of value. And if the folks that you are referring to would satisfy that standard, those are people that we could pursue.

Senator MCCASKILL. Well, why would you give a false—why would you provide a number that is not really the number they are using for—what kind of good could there be?

I mean, I am trying to figure out, I am trying to think about arguing a case to a jury in a criminal courtroom. Under what possible scenario would somebody be providing a phony caller ID number that wasn't up to something nefarious?

Mr. BASH. Examples that are mentioned in the context of the rulemaking that the FCC did to implement these rules involved calls coming from a battered women's shelter. A call might need to be made out by someone who is living there to check on her children, and she is needing to protect the actual number from which she is calling.

Senator MCCASKILL. And the blocked number is not sufficient in those instances? You can't just block the number so people can't see what it is?

Mr. BASH. The example I gave you is what we have pointed to and what folks refer to as legitimate uses of spoofing caller ID.

Senator MCCASKILL. In the grand scheme of things, I can't imagine that that is not just a tiny, infinitesimal number of these that are being given out.

And I would certainly like—we are going to ask you to do some follow-up on this. But one of the follow-ups I would ask you to look at is, what do we need to do to strengthen the laws to go after the people that are providing these phony numbers? Because that is a huge part of the problem.

Mr. BASH. And just to add to that, one of the suggestions that our former chairman made in submitting a report to Congress on potential changes to the Truth in Caller ID Act was to give the FCC direct regulatory authority over so-called third-party spoofing providers. These are people who are providing a service to people to spoof numbers.

Senator MCCASKILL. Thank you very much.

Senator Heller?

Senator HELLER. Thank you. And thanks again, Madam Chairman, for holding this hearing, and for our witnesses, for your testimony. Appreciate that.

I would be surprised if there is anybody here in this room that hasn't at one time or another been subject to a telemarketing call. And I would submit that I have. That second recording that you did on extended warranties on vehicles, every time my vehicle gets to be about 4 or 5 years old, I get that phone call. And when you ask follow-up questions, they usually hang up on you when they find out that they can't deceive you.

And in most cases, the deception practice is that you are thinking that you are talking to the original maker of that vehicle, whether that is a GM product, Ford product, or Nissan product. You think you are talking to that company. You know, at least they give off that perception. Then you find out that they are not associated with that organization.

So I thought that was a great example of the type of deception that we hear and see all the time.

Mr. Bash, you did a great job in your testimony of coming up with overcoming some of the enforcement challenges that you guys face.

And I was wondering, Ms. Greisman, if you have other ways. What can we do here in Congress to help allow you to have more authority? Do you need more authority? I am going to ask the next panel, of course, the same question. But what do you need? What kind of enforcement challenges do you face that you need to overcome that Congress could help you with?

Ms. GREISMAN. Well, I dare mention the common carrier exemption. We do think it is more than a relic. The commission is on record for the past several years in support of its elimination, and I certainly share that view.

Senator HELLER. OK. OK.

I want to clarify the numbers. You know, you have testified a little bit, both of you, a little bit on the numbers, the challenges that you are faced with.

Can you quantify the cost of this problem, both in the numbers of calls that people are receiving today and the cost? I know the chairman mentioned some costs. Just so that everybody here and those that are viewing this have an idea how big this problem is.

Ms. GREISMAN. Sure. First, with respect to the numbers, we know that through our law enforcement action we have halted literally billions of illegal robocalls. And we know that from the cases we have brought.

We also know that from the cases that have concluded in the robocall and do-not-call area that courts have ordered, I think it is, $740 million in redress or disgorgement. That, of course, is court-ordered. So that is at least a baseline for the scope of the magnitude of the economic injury being caused by this.

Senator HELLER. Do you agree with those numbers, Mr. Bash?

Mr. BASH. Yes. And I just want to reiterate what I said in my testimony, that the two most recent actions that we took, just the particular months that we were looking at, for our enforcement actions, these two operators had placed approximately 6 million calls in just several months.

Senator HELLER. How many individuals in your office do you dedicate to enforcement of no calls, telemarketing scams like this?

Mr. BASH. In the Enforcement Bureau, we have a handful of lawyers that are dedicated to dealing with this particular problem. On the policy side, our Consumer and Governmental Affairs Bureau works to implement the rules and change the rules as needed per any action you may take on Capitol Hill or to harmonize our rules with those of the Federal Trade Commission.

Senator HELLER. Is there a bureau within the FCC specifically dedicated to telemarketing fraud?

Mr. BASH. There is not one that is specifically dedicated to that.

Senator HELLER. How about the FTC?

Ms. GREISMAN. At the Federal Trade Commission, telemarketing rule enforcement, combating telemarketing fraud is something that is engaged in throughout the bureau. It is, as I mentioned before, a top priority.

Senator HELLER. Right.

Ms. GREISMAN. And it is not just the bureau at headquarters. Every regional office is involved in the fight against illegal telemarketing. The shop that I head is the manager/coordinator, if you will, of the telemarketing fraud enforcement program.

Senator HELLER. Thank you. I will preserve questions for later.

Senator MCCASKILL. Thank you.

Let me ask just a couple more things.

I want to make sure that it is clear how technology is changing this landscape. I think everyone has figured out that Congress is not nimble and we do not move quickly, and clearly we are behind the eight ball in many areas as it relates to technology.

And both of the agencies you work for have a very difficult job, because you are trying to get everyone to hold hands and sing "Kumbaya" when there are competing commercial interests and just competing interests because of advancing technology.

This is an area where most average Missourians don't understand why there is a different set of rules for the phone that rings in their house and the phone that rings in their purse. They don't understand why you can take action against a political campaign that calls the phone in the purse but you can't take action against the political campaign that calls in the family room when you are eating dinner.

And so would you explain why there would be these different rules? And try, if you can—I have a hard time with figuring out—I know it all boils down to wired versus wireless, and in the old days when everyone was paying by the minute as opposed to the vast majority of plans now that are not—well, there are still plans that pay by the minute.

But, you know, I don't think people—and then you have VoIP, which is, of course, the new method of phone calls that is not the common carriers but it is a wire nonetheless at some point. And where do they fall in this? And why should these rules all be different?

Ms. GREISMAN. I will take a stab and then turn it over to Mr. Bash.

From the FTC's perspective, it doesn't matter where the call rings. It doesn't matter whether it is at your home landline or in a device in your car, on your cell, wherever you are. It makes no difference; the telemarketing sales rule applies equally. And it doesn't matter whether it is coming over a copper wire or through the Internet.

With respect to the charitable calls that you mentioned, the FTC does not have jurisdiction over those bone fide charitable fundraising calls. We are able to reach for-profit telemarketers who place calls on behalf of bona fide charities, however.

Senator MCCASKILL. Right. So the people that call me that pretend that they are really helping the sheriffs and they are really taking 90 cents on the dollar and giving the sheriffs 10 cents, can you go after them?

Ms. GREISMAN. We can, and we have.

Senator MCCASKILL. OK.

Mr. BASH. So, as you heard me testify this morning, our rules do make a distinction between wireless phones and residential

landlines. And the distinctions that our rules make flow directly from the Telephone Consumer Protection Act of 1991.

Senator MCCASKILL. That is obviously up-to-date.

[Laughter.]

Mr. BASH. Maybe you will revisit that. But that is why our rules make the distinction that they do. The statutory language is really quite prescriptive, so our rules just track what the legislative distinctions in the law are.

And, as Lois was saying, with respect to VoIP, that is not really germane to the issue, because what matters is who is calling. It doesn't matter whether they are calling over VoIP or they are calling over a traditional telephone line. If you are making a call under the circumstances that are not legal, then it is impermissible.

Senator MCCASKILL. I think we have to really take a look at updating all of this so that, you know—there is a whole generation that is going to be very blessed by the fact that they can't get political robocalls, because none of my kids have landlines. And, you know, they were really glad last October in Missouri, because it was ugly out there.

But the elderly that are still answering that landline every day—I had a hard time. I felt like I needed this when I would go out in public, because everybody was so mad about these stupid political robocalls.

Let me just finally ask your thoughts—it seems to me that you are playing Whac-A-Mole. And you are playing Whac-A-Mole with people that many times are in foreign countries, and the long arm of the law is really, really difficult in these circumstances, especially since they can make a lot of money and shut down fairly quickly and move on. And your limited tools in law enforcement do not allow you to be as quick as they are, in terms of being able to get to them before they have shut down and moved on to another location or another IP address.

Talk a little bit about the technological solution. And what are the barriers that are in this country for—I mean, I know, I look at the technology that is available. I marvel at what I can do on this little, bitty box. I can run my life, literally, with this little, bitty box.

It is so hard for me to believe that there is not the technology available yet in America that we can control this without the government having a great deal of involvement, just through a technological answer.

And if you could speak to that briefly before we hear from our second panel, unless Senator Heller has more questions.

Ms. GREISMAN. I would be happy to start.

It is precisely because we felt there would be a technological solution that we launched the challenge. And the goal was to spur innovation, to tap into the genius of American consumers to develop ideas.

And I think it was enormously successful. There were three winners. But it is not just those three winners who submitted proposals that might go to market; there are others out there. And I think you will be very encouraged when you hear from Mr. Foss on the second panel.

Senator MCCASKILL. Great.

Senator Heller?

Senator HELLER. Thank you.

Mr. Bash, you talked a little bit about where these calls originate from. And I was wondering if you have any quantitative numbers of whether most of these robocalls are coming domestically or they are coming from foreign sources.

Mr. BASH. I don't think I have data to give you on that. I think that——

Senator HELLER. Do you have a feel for it?

Mr. BASH. I don't want to go out on a limb for that.

Senator HELLER. OK.

Mr. BASH. But I think it is fair to say that they are coming from both places.

Senator HELLER. OK.

Mr. BASH. They are coming from both places.

Senator HELLER. All right.

Ms. Greisman, you talked about enforcement challenges. And one of the things, of course, that you asked for is to abolish the common carrier exemption. And, of course, that would protect carriers from dual regulations by both the FCC and the FTC.

I guess my question to you is, is there any evidence or allegations that these common carriers are the source of these calls?

Ms. GREISMAN. Let me address that this way. From where we sit, we think common carriers can do two things. One is they can be more proactive in looking at what is going across their transom and flagging what probably are red flags.

We have some concerns that there may be some carriers out there—and remember, there is a real blurred distinction, given convergence in technology, of what is a telemarketer and what is actually a carrier. But we think there is some conduct that may be engaged in by some entities that purport to be carriers that would do more than raise an eyebrow.

Senator HELLER. OK. OK. I will probably ask the next panel the same question.

Mr. BASH. If I could add——

Senator HELLER. Please.

Mr. BASH.—on that subject, as I have mentioned in my written testimony, we obviously work with the Federal Trade Commission in coordinating law enforcement. And Lois and I, actually, just last week met on various coordination issues and issues with respect to carriers that she is aware of. She has made us aware of them, and we are certainly going to be looking at some of the information that was shared with us.

Senator HELLER. Terrific.

Thank you for your time. I want to thank both witnesses for being here.

And, Chairman, thank you very much.

Senator MCCASKILL. Thank you.

I am just curious, what is the conduct that raises the eyebrow? If you can tell us.

Ms. GREISMAN. It is too soon at this point to get into.

Senator MCCASKILL. OK.

Ms. GREISMAN. Thank you.

Senator MCCASKILL. I will be waiting.

[Laughter.]

Senator MCCASKILL. Thank you both.

And if the next panel would come forward.

I want to thank this panel. We have Mr. Kevin Rupy, Senior Director of Law and Policy, United States Telecom Association; Mr. Michael Altschul—am I saying that correctly?

Mr. ALTSCHUL. Yes, you are. Thank you.

Senator MCCASKILL.—Altschul, Senior Vice President and General Counsel at CTIA—The Wireless Association; Mr. Matthew Stein, Chief Technology Officer from Primus Telecommunications—welcome; thank you for being here—and Mr. Aaron Foss, Freelance Software Developer, Nomorobo.

Thank you, Mr. Foss. We are glad you are here.

And we will begin with your testimony, Mr. Rupy.

STATEMENT OF KEVIN RUPY, SENIOR DIRECTOR, LAW AND POLICY, UNITED STATES TELECOM ASSOCIATION

Mr. RUPY. Chairwoman McCaskill, Ranking Member Heller, thank you for giving me the opportunity to appear before you today. My name is Kevin Rupy, and I serve as Senior Director of Law and Policy at the United States Telecom Association.

U.S. Telecom and our member companies share the Subcommittee's concern about the problems associated with illegal robocalls. We understand the consumer frustration they cause, and we have long worked and coordinated with relevant private and government stakeholders to address this issue.

In addition to the harm they cause consumers, robocalls impact U.S. Telecom's own member companies. Our companies' customer service representatives represent the first line of defense on this issue. They must be well-versed in explaining to customers the difference between legal and illegal robocalls, providing them with information on how to file a complaint with the FTC, and pointing them to tools to help them mitigate these calls.

Robocalls can also adversely impact our companies' networks. Mass-calling events are typically highly localized, high-volume, extremely brief, lasting only a matter of minutes. And carriers receive no advance warning of these calls. A severe mass-calling event can result in service degradation and disruptions to phone services in a provider's impacted area. Moreover, illegal robocalls exacerbate an already troubling problem in our industry known as phantom traffic: calls that evade the established intercarrier compensation regime.

Given these impacts on both our customers and our networks, we can sympathize with the frustration you must feel at the apparent growth of this problem over the last 2 decades in spite of repeated legislative efforts to put an end to it. Those efforts illustrate the difficulty of keeping the law ahead of the lawbreakers and ahead of technology.

This is not to say that network operators are passive observers. As mentioned earlier, we serve on the front lines of defense and work in many other ways to monitor, mitigate, and respond to this problem. Many U.S. Telecom member companies maintain network operations centers that monitor network traffic, conduct traffic data forensics, and initiate mass-calling investigations.

Our members provide and will continue to develop various services, such as anonymous-call blocking, and other functionalities that help mitigate the problem. Network operators also work within standards-setting groups to address issues related to robocalls.

Carriers initiate legal actions against robocallers when they can be found and coordinate with state and Federal law enforcement agencies during ongoing investigations and enforcement actions.

Looked at through the lens of history, the explanation for this is regrettably fairly simple. The original phone network was a closed system, meaning that voice service was generally provided by local exchange carriers and long-distance companies through only the public switched telephone network, or PSTN, providing plain old telephone service.

Today's communications services are provided not by the historical closed PSTN but by a network of networks. The interdependent, interconnected, and global nature of the Internet means that areas of vulnerability exist throughout the network and, therefore, cannot be realistically addressed by any single stakeholder.

U.S. Telecom supports the development of possible technological solutions to the robocall problem by stakeholders throughout the Internet ecosystem, most of whom do not face the significant legal limitations outlined in my written statement that currently constrain our member companies.

But it is unlikely that any single technological silver bullet can permanently address the robocall problem. Today's solution could very well turn into tomorrow's Maginot Line and could have unintended adverse consequences, some examples of which I also outline in my written testimony.

The same increasingly appears to be the case for legislative and regulatory solutions, which regrettably do not seem capable of keeping pace with the evil genius of scammers, who continually invent new ways of evading discovery and capture, much less prosecution and punishment.

In closing, let me again thank the Subcommittee for holding this timely hearing. We share both the Subcommittee's and consumers' frustration, and we look forward to our continued work together in a manner that provides flexibility in addressing this constantly evolving challenge.

[The prepared statement of Mr. Rupy follows:]

PREPARED STATEMENT OF KEVIN RUPY, SENIOR DIRECTOR, LAW AND POLICY, UNITED STATES TELECOM ASSOCIATION

Chairwoman McCaskill, Ranking Member Heller, Members of the Subcommittee, thank you for giving me the opportunity to appear before you today to present the views of our industry on the burgeoning problem of robocalling. It is both timely and appropriate that the Subcommittee take time to review this important consumer protection issue. The United States Telecom Association (USTelecom) and our member companies are aware of the growing problem associated with illegal robocalls. We understand the consumer frustration they cause, and as a result we have long worked collectively and coordinated with relevant private and government stakeholders to address this issue.

My name is Kevin Rupy, and I serve as Senior Director of Law and Policy at USTelecom. Our association represents innovative broadband companies ranging from some of the largest companies in the U.S. economy to some of the smallest cooperatives and family-owned telecom providers in rural America. Our members offer a wide range of communications services on both a fixed and mobile basis, and the overwhelming majority of them offer advanced broadband services including voice,

video, and data. The customers that rely on our networks include consumers, businesses large and small, and government entities at the local, state, and Federal levels.

Robocalls are a Problem for Consumers and Providers of Voice Services

USTelecom's member companies are all too aware of the increasing consumer frustration attributable to robocalls. Probably all of us in this room have experienced such calls. They are intrusive and disruptive. That's bad enough. But through some calls' deceptive pitching of phony products and services such as debt reduction programs and mortgage modification scams, the criminals behind these calls are stealing money from unsuspecting consumers. Just last month, the FTC filed a complaint against one robocaller targeting current and former U.S. military members.

In addition to the harm they cause to consumers, robocalls impact USTelecom's own member companies. Often, the first call a consumer will make following a robocall incident is to the phone company. Our member companies' customer service representatives represent the first line of defense on this issue, and must be well versed in explaining to customers the difference between legal and illegal robocalls, pointing them to tools available to help them mitigate these calls and providing them with information on how to file a complaint with the FTC.

Robocalls can also adversely impact our companies' networks. Mass-calling events are typically highly localized, tremendously high volume, and extremely brief—lasting only a matter of minutes. And providers receive no advance warning of these calls. A severe mass-calling event can result in service degradation and disruptions to phone services in a provider's impacted area. Moreover, illegal robocalls exacerbate an already troubling economic problem in our industry because they can often be associated with "phantom traffic"—calls largely originating outside our companies' local calling areas for which a terminating access charge will never be paid by the long-distance carrier because the necessary call identification information has been stripped.

What Are Robocalls and Why Have They Proliferated?

The proliferation of robocalls has resulted from three major changes in the communications marketplace. The global reach of the Internet, combined with the widespread availability of mass-calling technology and a dramatic reduction in the costs of long-distance service, have radically changed the capabilities and economics of robocalling. As former FTC Chairman Jon Leibowitz stated at last October's FTC-sponsored robocall workshop, the Internet has allowed "voice blasting technology to flourish at bargain basement prices."

Looked at through the lens of history, we can sympathize with the frustration you must feel at the apparent growth of this problem over the last two decades in spite of repeated legislative efforts to put an end to it. Those efforts illustrate the difficulty of keeping the law ahead of the law-breakers—and ahead of technology. The Federal Trade Commission (FTC), over which this Subcommittee has jurisdiction, was specifically directed under the Telemarketing and Consumer Fraud and Abuse Prevention Act of 1994 to adopt rules prohibiting deceptive and abusive telemarketing acts or practices, including "unsolicited telephone calls which the reasonable consumer would consider coercive or abusive of such consumer's right to privacy." The body of regulations adopted by the FTC to implement this 1994 Act is known as the Telemarketing Sales Rule. The FTC is also empowered generally to address unfair or deceptive acts or practices in or affecting commerce, which the Federal Trade Commission Act declares unlawful. But the FTC's jurisdiction does not extend to common carriers, which are subject to the regulatory authority of the Federal Communications Commission (FCC). And for reasons described below pertaining to both our common carrier and privacy obligations, our member companies must complete phone calls.

Viewed from the perspective of communications law, when Congress adopted the Telephone Consumer Protection Act of 1991 (TCPA) to address telemarketing robocalls, its major purposes were to protect the privacy and public safety interests of telephone subscribers by placing restrictions on automatic dialers, fax machines, and unsolicited automated calls. The TCPA amended Title II of the Communications Act of 1934 to add a new section 227, entitled "Restrictions on the Use of Telephone Equipment." The nature of the technology being used in 1991 is well-illustrated by a consumer complaint listed among several examples in this Committee's report accompanying the bill (S. Rept. 102–178): "the automated calls filled the entire tape of an answering machine, preventing other callers from leaving messages." Except for amendments to expand the reach of section 227 to offshore callers and to prohibit caller-ID spoofing, the robocall provisions of the law remain largely as

they were enacted in 1991—and, as we all know, they have become increasingly ineffective.

The explanation for this is, regrettably, fairly simple. The original phone network was a "closed" system, meaning that voice services were generally provided by local exchange carriers and long distance companies through only the public switched telephone network (PSTN). These companies were providing what is called "plain old telephone service," or POTS. When Congress passed the TCPA in 1991 to address robocalls, autodialing systems, and certain fax machine problems, and even when it acted again three years later to deal with unsolicited telemarketing calls, wireless communication was only beginning to emerge and even dial-up Internet access was not yet a reality for mass consumer use. In contrast to the situation that confronted Congress in the early 1990s, today's communications services are provided not by the historical closed PSTN but by a "network of networks."*

As a result, voice service is now available from a myriad of companies with a diverse technical heritage. We still have the PSTN, but we also have Voice over Internet Protocol (VoIP) providers, Internet service providers, and cable companies offering "phone" service, right alongside competitive local exchange carriers and wireless carriers. Approximately 40 percent of U.S. households have "cut the cord" and rely entirely on wireless for their voice service. And by the end of 2013, USTelecom estimates that more than 52 percent of wireline households will subscribe to interconnected VoIP, oftentimes provided by the local cable company. Finally, "over-the-top" VoIP services—which use existing broadband networks—are widely available to American consumers and are offered by some of the country's most prominent companies, including Vonage, Google Voice, and Microsoft's Skype service. Skype, for example, disclosed to the Securities and Exchange Commission in August 2010 that the company had 20 million connected users in the United States, 1.9 million of whom were paying customers.

Regardless of their delivery platform, each of these voice providers must ultimately connect to the PSTN because the reliability of their service to their own customers depends on their ability to deliver any call to anywhere. As a result, "phone" calls can connect to anyone, anywhere, regardless of whether a consumer's phone is connected to the PSTN, or their wireline or wireless phone or computer is connected to a broadband network. But this same remarkable connectivity—a connectivity we celebrate and want to expand to those Americans who don't yet enjoy it—also makes it possible for robocalling con artists and fraudsters to set up shop virtually anywhere in the country or even the world and, with the right equipment and a few clicks of the mouse, begin auto-dialing unsuspecting and vulnerable consumers across the United States.

The Contextual Nature of Robocalls—What the Consumer Sees

Now that we understand the network framework under which robocalls operate, it is important to understand the various types of robocalls. It can be helpful to consider all mass calling and robocall events as a traffic signal, comprised of green, yellow, and red lights. Robocalls that are important and legal would fall into the "green" category; robocalls that are legal, but whose usefulness are a matter of subjective personal opinion, would fall into the "yellow" category; and malicious and illegal robocalls would fall into the "red" category.

So, for example, a consumer may receive a "green" robocall from his or her child's school, stating that the school's opening will be delayed due to bad weather. Similarly, public safety agencies will often use robocalls to provide critical public safety messages. For example, Los Angeles County has implemented an emergency mass notification system used by the County's Emergency Operations Center to notify residents and businesses of emergencies or critical situations and provide information regarding necessary actions, such as evacuations due to wildfires. Because the system uses geomapping, emergency notifications can be directed to very specific geographic areas. Clearly, robocalls of this type would fall into the "green" category.

Robocalls falling on the "yellow" spectrum are also legal, although some recipients might be indifferent to their messages or might prefer not to receive them. A doctor's office may use a robocall to remind a patient of an upcoming appointment. Similarly, political candidates and political groups will often use robocalls to solicit votes in an upcoming election, or to deliver an advocacy message.

Finally, there are the instances of illegal calls falling into the "red" category of calling events. These calls include the infamous "Rachel from Card Services," as well as other bogus schemes selling everything from cruises to insurance.

---

*To put this in further perspective, the first website was created in 1991—the year of the TCPA's enactment. Today, there are more than 30 trillion individual web pages.

Robocallers are becoming increasingly creative in perpetrating their scams, many of which originate from beyond our Nation's borders.

The traffic from a robocaller directed toward a consumer on the PSTN can transit the network either over the Internet, or through the PSTN itself. In fact, it is usually the case that a typical mass-calling event will transit multiple networks—encompassing both the PSTN and the Internet—before finally reaching the consumer.

The Contextual Nature of Robocalls—What the Service Provider Sees

Consumers are the only ones who can ultimately determine the nature of any specific robocall. Service providers, conversely, have no visibility into the specific nature or type of robocall transiting their network. They have no way of determining whether the call is illegal or legal. The service provider may only see that a mass calling event is taking place at a specific point on their network.

From the service provider's perspective, these mass calling events are defined by four characteristics. First, they are highly localized in nature. Second, they are represented by a high volume of calls. Third, once the calls arrive at their intended local target, they are extremely brief—potentially only lasting a matter of seconds or minutes. Finally, there is no advance warning for these calls.

Adding further complexity to the robocall issue is the problem of caller-ID spoofing—misrepresenting one's identity using a deceptive caller-ID. Although, after the fact, providers have investigative techniques that can positively identify whether a call has been spoofed or not, there is no way for a carrier to make that determination in real time, as the call is transiting the network.

Significant Legal Constraints Limit Potential Robocall Deterrents

Two primary legal issues face USTelecom's member companies with respect to remedying the robocall problem. First, under existing laws to which USTelecom's members are subject for their provision of legacy voice service, 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 our companies to decide for the consumer which calls should be allowed to go through and which should be blocked.

Second, there are substantial privacy issues that arise in any discussion relating to proposed robocall solutions. Robocalls are extremely contextual in nature. Depending on the nature of the call, certain robocalls are permitted under the law, while others are prohibited. Proposed solutions to the robocall dilemma that seek to make phone service providers the arbiter of whether a call should—or should not—be permitted to proceed skirt dangerously close to violating the privacy obligations imposed on us by law. For example, the Wiretap Act (also known as Title I of the Electronic Communications Privacy Act (ECPA) or Title III of the Omnibus Crime Control and Safe Streets Act of 1968) expressly protects wire, oral, and electronic communications while in transit and establishes that service providers are permitted to intercept those communications only as a necessary incident to the rendition of service or to the protection of the rights or property of the provider. Similarly, except as authorized by ECPA, section 705 of the Communications Act of 1934 makes it a crime for any person "to intercept and divulge or publish the contents of wire and radio communications"—a provision not limited solely to common carriers.

The Practical Realities of Technological and Legislative Solutions

The interdependent, interconnected, and global nature of the Internet means that areas of vulnerability exist throughout the network, and therefore cannot be realistically addressed by any single stakeholder. Given the rapid and ever-changing nature of the robocall problem, it is highly unlikely that a technological "silver bullet" can be developed as a permanent solution. Much in the same way that remediation efforts in areas such as spam or cybersecurity must continually evolve, the same can be expected for robocalls.

Robocalls, like their brethren in the area of spam, phishing, and cybersecurity is a constantly evolving problem. USTelecom supports the development of possible technological solutions to the robocall problem by stakeholders throughout the Internet ecosystem, most of whom are not constrained by the significant legal limitations currently facing our members. But members of this Subcommittee need to be aware that no single solution will permanently address the robocall problem. Today's solution could very well turn into tomorrow's Maginot Line, and could have unintended adverse consequences.

For example, solutions that rely extensively on blocking calls populated by a blacklist could very well result in the blocking of legitimate calls from callers whose own phone numbers have been illegally spoofed. Conversely, solutions implementing

call blocking features based upon a whitelist could potentially block an important—albeit unexpected—message from a legitimate caller. Even more perversely, the availability of spoofing technology can easily fool consumers into taking calls they should avoid. For example, spoofing the number of the local municipal hospital could dupe a senior citizen into believing that a fraudulent effort to sell phony medical products is actually a legitimate call from a whitelisted number. Given the open nature of the broadband network, technological solutions can be—and often are—superseded by technological countermeasures.

The same increasingly appears to be the case for legislative and regulatory solutions, which regrettably do not seem capable of keeping pace with the evil genius of scammers who continually invent new ways of evading discovery and capture, much less prosecution and punishment. As noted earlier, we have been trying to legislate out of existence the problems of robocalling, spam, autodialing, and caller-ID spoofing for as long as two decades, but new technologies only seem to make the problems grow worse.

Addressing Robocalling Requires A Multi-Pronged Approach

This is not to say that carriers are passive observers to the robocall problem. USTelecom's member companies work on multiple fronts in order to monitor, mitigate, and respond to mass-calling events. For example, many USTelecom member companies maintain network operations centers (NOCs), which include 24-hour security desks that monitor network traffic, respond to consumer complaints, conduct traffic data forensics, and initiate mass calling investigations.

In addition, carriers are providing—and will continue to develop—various services consumers can use to help mitigate the robocall problem. These services include basic caller-ID functionality, as well as conditional call-forwarding and anonymous call-blocking. Because the offerings and capabilities of companies are different, consumers are always encouraged to contact their respective service provider in order to identify available resources.

Network operators also work within the framework of various standards setting groups, the best example of which is the Alliance for Telecommunications Industry Solutions (ATIS). ATIS is a standards organization that develops technical and operational standards for the communications industry, including standards related to the handling of mass-calling events. In addition, several USTelecom member companies are members of the Communications Fraud Control Association (CFCA). CFCA's membership consists of approximately 200 different carriers, private network owners, end users, law enforcement officers, and others from around the world. Through these public-private partnerships, industry stakeholders work together to identify best practices and solutions to a broad range of telecommunications-related issues, including robocalls.

Carriers will initiate legal actions against robocallers when they can be found and coordinate with law enforcement agencies at the state and Federal level during ongoing investigations and enforcement actions. For example, in a 2010 FTC action against a robocaller that allegedly made more than 370 million calls to consumers nationwide in a single year, the agency specifically acknowledged the assistance that both AT&T and Verizon provided in the investigation of the case.

Finally, the competition between our companies and other communications platforms for consumer and enterprise business provides incentives for all communications providers to innovate and to develop new and more effective solutions to challenges such as robocalling. This competition requires us to offer consumers the best possible experience subject to what the law allows us to do, including taking action to mitigate robocalling. If we do not offer effective solutions, consumers will simply migrate to alternate technologies that offer better ones.

In closing, let me again thank the Subcommittee for holding this timely hearing. We share both the consumer's and Subcommittee's frustration with the issue, and we look forward to our continued work together in a manner that provides flexibility in addressing this constantly evolving challenge.

Senator MCCASKILL. Thank you, Mr. Rupy.

And I am going to interrupt here for a moment. We have been joined by Senator Pryor. And this is a subcommittee that really has overlapping jurisdiction with Senator Pryor's subcommittee on telecommunications. And so I would like to defer to him for a moment.

If you would like to make any comments at this point, Senator Pryor, before we continue with this panel, that would be terrific.

Thank you for joining us today. Between Consumer Protection and your committee—and I know you were the former chairman of this subcommittee, so I really appreciate you cooperating with us and allowing us to have this hearing even though we could argue about the jurisdiction, which we do around here sometimes, I have noticed.

[Laughter.]

STATEMENT OF HON. MARK PRYOR,
U.S. SENATOR FROM ARKANSAS

Senator PRYOR. That is OK. No, I am thrilled that you are chairing this subcommittee now. It is a great subcommittee, as you know, great staff and a great team of people here. But thank you.

Let me just say, we have a great leader in Chairwoman McCaskill. She is going to do great things with this subcommittee.

And these are very important issues that you are talking about today. And we may have had some overlapping jurisdiction, but I don't care, because I think that you are going to handle this hearing just great. And I just want to say thank you for your hard work, and I want to say thank you to all the Subcommittee members.

You know, I look at the numbers; it is clear that the Do Not Call Registry has been a success. And I am pleased that the FTC is working with states to crack down on the individuals with robocalls and other illegal activities.

So everybody is working together; we can solve this. So all I want to say is thank you. And I didn't want to interrupt, but thank you.

Senator MCCASKILL. Thank you, Senator Pryor.

Mr. Altschul?

STATEMENT OF MICHAEL F. ALTSCHUL,
SENIOR VICE PRESIDENT AND GENERAL COUNSEL,
CTIA—THE WIRELESS ASSOCIATION®

Mr. ALTSCHUL. Good morning, Chairman McCaskill, Ranking Member Heller, and Senator Pryor. On behalf of CTIA, thank you for the opportunity to participate in this morning's hearing to explore ways to protect consumers against unlawful robocalls and SMS text messages.

CTIA was proud to support initial adoption of the Telephone Consumer Protection Act back in 1991. In fact, I had just joined the association; it was one of the first legislative issues I worked on.

Like our customers, wireless carriers are also victims of illegal text message phishing scams and robocall campaigns by unscrupulous boiler-room operators seeking to sell extended car warranties and the like that violate the protections in the TCPA and other laws.

That is why CTIA has called on the FCC to change the way it reports TCPA complaints, which, as you may know, are divided into wireless complaints and wireline complaints. These consumer complaints are about calls and messages that originate outside of a carrier's network and control. And the way the FCC reports them actually tends to hide the magnitude of the problem in their reports.

CTIA and our member companies understand consumer annoyance over these calls and repeatedly have pledged our full cooperation to efforts by the FCC and the FTC to bring enforcement actions against robocallers and fraudsters who violate the TCPA.

In cases where they can locate and identify the source of the messages, our carrier members have brought lawsuits against the perpetrators. And the industry has cooperated with the FTC and state attorneys generals in their investigation and prosecution of these cases.

However, as you have heard from other witnesses, it is virtually impossible to trace an interconnected VoIP call or an over-the-top text message delivered to a wireless carrier from the Internet, especially when the sender wants to disguise his or her identity through the use of proxy servers and spoofed caller ID.

I would like to use a screenshot of a text message that I received on Monday to illustrate the difficulties we face in trying to solve this problem.

And, by the way, wireless carriers do screen text messages and successfully block millions of them, I believe, every day. Voice calls have to be found at the source to be cut off.

As you can see, this text message appears to be an informational text message about my account at a local financial institution. In fact, I have provided my express prior consent to the financial institutions where I have accounts, authorizing them to send me informational text message alerts about fraudulent activity, data breaches, and other time-sensitive account information.

But since I do not have an account at this institution, I knew immediately it was a phishing scam that violates both the TCPA and the Truth in Caller ID Act, which prohibits the spoofing of caller IDs. Scammers, especially those outside of the United States, are not deterred from violating the TCPA or the Caller ID Act.

For this phishing scam, the fraudster spoofed the caller ID of a local Washington, D.C., phone number. As it turns out, this number is not in service. It happens to be assigned and arranged so that it is assigned to a CLEC. But I called it and got a recording that the number is not service. So this is not a real phone number assigned to a user.

But the fraudster could just as easily spoof the financial institution's actual phone number or tumbled phone numbers randomly to defeat the use of blacklists and whitelists. And this is why this is such a difficult problem to solve. Carriers do not know the businesses and public agencies the customer has given express prior consent to send informational calls and messages. And even if a carrier did know this information, fraudsters can spoof whitelisted numbers and appear to be a legitimate business sending informational calls and messages to its customers.

We appreciate the efforts of the FTC and others who are exploring technologies that may minimize the transmission of illegal robocalls and text messages to our customers. However, as H.L. Mencken famously observed, there is always a well-known solution to every human problem neat, plausible, and wrong. This wise counsel cautions us that any technical solutions must be subject to careful and complete consideration.

So, on behalf of CTIA, thank you for your consideration of these suggestions. We look forward to working with you to address these and related matters as the Subcommittee moves forward.

[The prepared statement of Mr. Altschul follows:]

PREPARED STATEMENT OF MICHAEL ALTSCHUL, GENERAL COUNSEL, CTIA—THE WIRELESS ASSOCIATION®

Good morning Chairman McCaskill, Ranking Member Heller, and members of the Subcommittee. On behalf of CTIA—The Wireless Association®, thank you for the opportunity to participate in this morning's hearing to explore ways to protect consumers against unlawful robocalls.

Like our customers, wireless carriers are also victims of robocall campaigns by unscrupulous "boiler-room" operators seeking to sell extended car warranties and the like that violate the protections in the Telephone Consumer Protection Act (TCPA). At CTIA, we and our members understand consumer annoyance over these calls and repeatedly have pledged our full cooperation to efforts by the FCC and the FTC to bring enforcement action against these serial violators of the TCPA. In cases where they can locate and identify the source of these messages, our carrier members have vigorously brought suit against the perpetrators, and the industry has cooperated with the FTC in its investigation and prosecution of TCPA cases.

CTIA was proud to support initial adoption of the Telephone Consumer Protection Act in 1991. At that time, there were roughly seven million wireless subscribers in America, and nearly every wireless subscriber also had a landline phone. Today, there are more than 326 million wireless subscriber connections in the United States, including connections for advanced communications devices like smartphones and tablets that access increasingly ubiquitous wireless broadband services. The U.S. wireless industry now leads the world in delivering next generation wireless services. Wireless has evolved from a niche voice service to the primary source of broadband communications for millions of Americans. Consumers' mass migration to wireless-only service also is a testament to the attractiveness of wireless prices. According to the Bureau of Labor Statistics' Wireless Price Index, the effective monthly cost of wireless service to consumers has fallen more than 40 percent since December 1997.

At the same time, because of the real reduction in the price of a wireless call, the popularity of rates plans that offer "buckets" of minutes and unlimited calling on nights and weekends, innovative devices and applications, and the added convenience that wireless offers to consumers who value personal and untethered communications, a substantial portion of the population has moved or is moving to "cut the cord" and rely completely on their wireless phones as their only means of communication. Currently more than 35 percent of U.S. households are "wireless only" for their voice service, and the percentage is significantly higher in some regions and among certain segments of the population.

Of particular significance for today's hearing, the continuing trend to adoption of wireless service as the primary source of communications for millions of Americans, and the changes that have flowed from innovative rate plans and the greater affordability of wireless service, justify a fresh look at the TCPA's treatment of pre-recorded calls to mobile devices.

For instance, given the shift in the way consumers use their mobile devices the TCPA's disparate treatment of informational calls that depends upon whether a company is calling a wireline or wireless phone number—or, increasingly, a number associated with an interconnected VOIP provider that simultaneously forwards the call to a customer's wireline and wireless numbers—is increasingly out of date. As currently enacted, the TCPA requires the "prior express consent" of the called party for even informational calls to wireless phones if the calls are prerecorded or use an autodialer; non-commercial informational calls to residential phones are not similarly restricted. This disparity creates challenges for companies and government agencies that want to provide legitimate informational calls to individuals who are not reachable in any other way and who may value such calls to receive timely information such as notification about a data breach, fraud alert, change in flight time, or other time-sensitive account information.

Even where a consumer has given prior express consent to one entity to receive autodialed calls on her mobile device, that consent would not apply to informational calls from other entities about that purchase. For example, I may have given LL Bean consent to call me on my cell phone when I ordered a new shirt, but that would not permit UPS to notify me about scheduled delivery times. Similarly, I may have given the auto dealership consent to call my cell phone when I purchased my

car, but that consent may not extend to the auto manufacturer that wants to later call me about a safety recall.

A key adjustment to the TCPA that would help resolve this issue would be clarification of the statutory definition of an "automatic telephone dialing system" (ATDS), at least as it applies to delivery of informational calls. The TCPA defines an ATDS as "equipment which has the capacity to store or produce telephone numbers to be called, using a random or sequential number generator" and the ability "to dial such numbers." The Federal Communications Commission and some courts have interpreted this definition to include equipment that dials numbers from a list of customer phone numbers that are neither random nor sequential. The equipment simply aids the calling party by automating the process of dialing these intentionally selected numbers. This expansive interpretation potentially leaves wireless customers unable to receive desirable informational messages, like a fraud alert from their bank, while there remain no restrictions on sending the same alert message to the dwindling number of consumers that maintain a landline phone. A welcome clarification to the TCPA would allow use of ATDS to send informational messages to wireless phones, so long as they are not used to dial numbers sequentially or randomly.

Another outmoded aspect of TCPA implementation is the fact that the Federal Communications Commission continues to catalog consumers' TCPA reports as "wireless complaints," suggesting they are complaints about wireless service, when the complaints are in fact about violations of the TCPA and FCC rules by telemarketers calling consumers on their wireless phones. As I noted at the outset, wireless carriers have taken numerous steps—including bringing lawsuits against robocallers—to protect their customers against unlawful calling campaigns. At CTIA, we understand consumer annoyance over these calls and repeatedly have pledged our full cooperation to efforts by the FCC and the FTC to bring enforcement action against these serial violators of the TCPA.

Yet while wireless carriers are doing what they can to identify and shut down TCPA violations, the FCC continues to misleadingly catalog consumers' TCPA reports as "wireless complaints." We believe it is unfair for the FCC to continue to count TCPA complaints, which are about calls that originate outside of the wireless network and have nothing to do with wireless carriers' behavior, as "wireless complaints." The FCC's refusal to properly characterize these consumer complaints significantly and misleadingly expands the apparent rate of consumer complaints about wireless services. This is important since absent inclusion of TCPA-related complaints, the total number of complaints about wireless service received by the FCC has been declining significantly, dropping from 12/1000ths of one percent of industry subscribership in 2005 to slightly more than 7/1000ths of one percent today. To ensure accurate reporting, we believe the FCC should disaggregate TCPA data from its quarterly and annual wireless complaint data and report it separately.

Let me turn now to the question of whether technical solutions can help address the problem of unlawful robocalls. While the recent effort by the FTC to use a contest to identify a technical solution that would allow consumers to automatically screen and reject unwanted robocalls produced some interesting proposals, the limited information available to CTIA and the public about these proposals suggests the FTC and others should approach implementation cautiously.

Each of the three winning entries in the contest, including one submitted by two engineers at Google, relies on creation of a "blacklist" database of numbers identified as associated with robocall spammers. All incoming calls to a consumer would be compared with this database, with calls from blacklisted numbers blocked. The database would also include a "whitelist" of numbers associated with entities that have been identified as associated with "legitimate" callers. While there may be value to these solutions, they raise a number of issues that would need to be resolved before any such system can even be considered for implementation.

- *Identification of Blacklist Numbers.* Each of the proposed systems includes a method for identifying numbers to be included on the blacklist—some using consumer input and at least one using a mathematical algorithm. But there are significant issues with either method. Given the ease with which robocallers using modern equipment can mimic the caller ID of any other phone user, a consumer or an algorithm may think it is identifying an illegal robocaller for the blacklist, when it is actually listing the number of an innocent party. Illegal robocallers can also change the numbers they use (or the numbers they mimic) frequently—even "tumbling" a new legitimate number for each individual robocall—limiting the usefulness of the blacklist. This suggests a need to contact the person or business associated with the number in order to provide an opportunity to object to being placed on the blacklist. Would there be an appeal

process? Would there be criteria for moving an innocent customer from the blacklist to the whitelist? In addition, one person's unwanted annoying robocall may be another person's important informational message. One consumer may suggest adding a political candidate's number to the blacklist because he or she is annoyed with the candidate's message, while others may welcome such messages. It is unclear how an algorithm could even distinguish between wanted and unwanted robocalls.

- *Identification of Whitelist Numbers.* Before implementation, rules would need to be worked out and a system administrator appointed to determine how, and on what basis, a robocaller could get its number added to the whitelist. Would there be an appeal process? What would be the criteria for moving a bad actor from the whitelist to the blacklist?
- *Caller ID Spoofing.* Even assuming an accurate database of blacklisted and whitelisted numbers can be compiled and maintained, the ease with which modern equipment and software can allow a caller to hide its identity by spoofing a caller ID would present significant challenges. It would, for example, be relatively simple for an illegal robocall spammer to spoof one or more of the numbers on the whitelist to get its calls through the protection system. While the Truth in Caller ID Act prohibits spoofing of caller IDs for fraudulent or harmful purposes, unlawful robocallers—especially those that are calling from outside the United States—that aren't deterred from violating the TCPA would likely have little concern about also violating the caller ID law. Identifying illegal robocallers that are spoofing caller ID is made significantly more difficult if the robocaller uses modern Voice over Internet Protocol (VOIP) technology, which if routed through a proxy server becomes virtually impossible to trace.
- *Scaling.* Because unlawful robocallers typically use a large number of telephone numbers and change telephone numbers frequently, the database for the blacklist would be very large and continually growing, requiring a significant investment for both acquisition and maintenance of computer resources. Perhaps more significantly, the capacity in both telecommunications and computer resources needed to route to the database for comparison all of the calls robocallers may make to the tens or even hundreds of millions of persons who may sign up for the service would be massive.
- *Administration and Operation of the System.* Any robocall blocking system of the type proposed in the FTC contest would involve a fairly massive administrative and operational effort. It should not be expected that carriers can be the implementing entities. The significant costs of the system aside, a single carrier could reasonably compile and maintain a robocall blacklist that would be associated only with the illegal robocall identification and calling preferences of its own customers. Thus no system operated by a single carrier could be as comprehensive as it would need to be to be effective. In addition, wireless carriers, as legal common carriers, must deliver calls that are placed on their networks. While a subscriber that opted in to the proposed robocall blocking system may be considered to have authorized the blocking, the carrier may not block calls from a legal robocaller on its network, absent specific statutory or regulatory authority to do so.
- *Privacy Issues.* At least one reported robocall solution would require the carrier to allow the solution administrator to screen subscribers' incoming calls to determine whether they are from an illegal robocaller or a legal robocaller or live individual. Even if this kind of snooping is authorized by the recipient of the call, such a potentially invasive technology raises serious questions about consistency with the law and rules governing the privacy of customer proprietary network information and a carrier's traditional responsibility to avoid intercepting or divulging the content of communications other than in narrowly circumscribed instances.

We appreciate the efforts of the FTC and others who are exploring technologies that may minimize the transmission of illegal robocalls to our customers. As the foregoing suggests, however, any technical solutions must be subject to careful and complete consideration. Particularly at this early stage of development, it would be premature to impose any technical solution as a mandate.

Finally, whether as part of a technical solution to robocalls or as part of any amendment to the TCPA, nothing should be done to upset the FCC's longstanding conclusion under the TCPA that wireless carriers need not obtain additional consent from subscribers prior to initiating autodialed calls at no cost to their subscribers. These important and beneficial customer service calls may be used to notify customers of billing alerts, low balance alerts on prepaid phones, and usage alerts in-

forming customers of approaching limits for voice, data, or messaging plans. In encouraging wireless carriers to provide this information to their customers, the FCC has consistently recognized the benefits of such calls between wireless carriers and their customers and recognized that Congress had no intention of hindering these communications. Any new solution to illegal robocalling, whether technical or through increased enforcement, should not upset this key communication between wireless providers and their customers.

On behalf of CTIA, thank you for your consideration of these suggestions. We look forward to working with you to address these and related matters as the Subcommittee moves forward with its work.

Senator MCCASKILL. Thank you very much.

Mr. Stein?

STATEMENT OF MATTHEW STEIN, CHIEF TECHNOLOGY OFFICER, PRIMUS TELECOMMUNICATIONS INC.

Mr. STEIN. Thank you, Chair, Ranking Member Heller, and Senator Pryor. My name is Matthew Stein, and I am the Chief Technology Officer of Primus Telecommunications. While my responsibilities at Primus cover all of our technology assets globally, my comments today are specific to our Canadian business, known as Primus Canada.

As in the United States, robocalls are a concern in Canada, and I thank you for the opportunity to speak to a technological solution invented, developed, and deployed by Primus.

Primus provides a service called Telemarketing Guard to all of our telephone customers in Canada. This patented service was developed and deployed in 2007 in response to our customers' discontent with their inability to control unlimited, unsolicited calling.

The concerns expressed by our customers are familiar: unwanted calls interrupting dinner, interrupting quiet evenings, interrupting family time, and, in many cases, the inability to make these calls stop, no matter how many times the customer asked to be taken off one kind of list or to be put on another.

Before I proceed, it is important to make clear that we view robocalls and automated telemarketing calls as a subset of mass unsolicited calling, which, for convenience, I will refer to as "telemarketing." Our customers have made clear that their view of telemarketing does not change if they are greeted by a live person or a recorded message when they pick up the phone.

Telemarketing Guard addresses this issue by providing customers with control over how they wish to deal with telemarketing calls. When a call is placed to a customer protected by it, our system evaluates the call even before the phone has rung. If the system believes, based on feedback provided through our customers, that the caller is likely a telemarketer, the call does not go directly to our customer. Instead, a message is played telling the caller that the customer does not accept telemarketing calls and invites them to press "1" to record their name so that their call can be announced. The customer then has the choice to accept the call, refuse the call, or send it to voice-mail, all without actually speaking to a telemarketer.

Telemarketing Guard uses the actions of our customers to identify these telemarketing calls. The system is completely neutral to all phone numbers until a report from a customer is received. As a result, all calls, telemarketing or not, are unimpeded to our cus-

tomers initially. But if a customer receives an unscreened telemarketing call, it is up to them to decide whether or not they will choose to report that number, which they can do by picking up their phone and dialing a special code.

If they choose to report the call and if a threshold of other customers also reports that call, the system begins to monitor the phone number and scans for a number of behavioral characteristics. For example, these could be frequency of calling, time-of-day concentration, sequential calling, and so on. There are many, many other elements that are scanned for. All of this is done to determine if the call should be identified as a telemarketer on a go-forward basis.

In essence, the system promotes and relies on customer engagement to identify telemarketing calls. But the reverse is also true. If enough customers accept a call from an identified telemarketer, the number will cease to be considered a telemarketer by the system.

This is accomplished by a system that requires no arduous maintenance of lists or complicated judgment calls to be made, whether by network providers, by third parties, or government bodies. Instead, the system just tallies customer votes to determine who is and who is not an unwanted telemarketer. In other words, it becomes a living, breathing, crowdsourced list of undesirable telemarketers and robocallers.

Further, customers that don't even bother to participate in reporting still benefit from the actions of those that do. This is the defining element of Telemarketing Guard and what we believe makes it unique. In fact, this is what led us to patent this system.

Customer engagement and response have been exceptional. Based on our internal surveys, the service has increased customer satisfaction and become one of the leading reasons customers choose to keep their phone service with Primus.

In regards to costs and implementation, the system is not complicated or expensive to establish and maintain. Indeed, we currently provide Telemarketing Guard to all of our customers at no extra charge. The system can also be grafted easily into existing phone networks, as we did into ours. It can work for traditional landline phones, Voice-over-IP phones, or mobile phones. The service doesn't require customers to buy anything or install anything or configure their phone in certain ways. And, finally, the service itself can be adapted and configured to address needs of consumers, telephone service providers, or legislative and regulatory bodies.

In conclusion, besides being a powerful consumer tool, we believe that Telemarketing Guard is consistent with the competitive interests of telecommunications carriers to provide valuable new services to customers. Primus therefore welcomes the efforts of this committee to identify ways that consumers can be given more tools to address mass unsolicited calls and to encourage carriers to provide such services.

Thank you, and I look forward to any questions you may have.

[The prepared statement of Mr. Stein follows:]

PREPARED STATEMENT OF MATTHEW STEIN, CHIEF TECHNOLOGY OFFICER, PRIMUS TELECOMMUNICATIONS INC.

Thank you Chair and distinguished members of the Committee. My name is Matthew Stein, and I am the Chief Technology Officer of Primus Telecommunications Inc. While my responsibilities at Primus cover all of our technology assets globally, my comments today are specific to our Canadian business, known as Primus Canada. As in the United States, robocalls are a similar concern in Canada and I thank you for the opportunity to speak to a technological solution invented, developed, and deployed by Primus to assist our customers with this issue.

Primus provides a service called Telemarketing Guard to all of our telephone customers in Canada. This patented service was invented in 2006, and deployed in 2007 in direct response to our customers' discontent with their inability to control and limit unsolicited calls. The concerns expressed by our customers are familiar—unwanted calls interrupting dinner, interrupting quiet evenings, interrupting family time and, in many cases, the inability to make the calls stop no matter how many times the customer asks to be taken off one kind of list or put on another.

Before I proceed, it is important to make clear that we view robocalls and automated telemarketing calls as a subset of mass unsolicited calling, which for convenience I will generally refer to as telemarketing calls throughout my presentation. Our customers have made clear that their view of telemarketing calls does not change if they are greeted by a live person or a recorded message when they pick up the phone.

Telemarketing Guard addresses this issue by providing customers with control over how they wish to deal with telemarketing calls. When a call is placed to a customer protected by Telemarketing Guard, our system evaluates the call even before the customer's phone is rung. If the system believes, based on feedback provided by our customers, that the caller is likely a telemarketer, the call does not go directly to our customer. Instead, a message is played advising the caller that the customer does not accept telemarketing calls and invites them to press 1 to record their name, so that their call can be announced to the party they are calling. After the caller records their name, similar to leaving a voice-mail, the system calls our customer and advises them that they have received a potential telemarketing call and plays the recording provided by the caller. The customer then has the choice to accept the call, refuse the call, or send the call to voice-mail if available. In fact, customers often decide to ignore the call altogether without even having to answer the phone as the caller ID will display the name "Telemarketing Guard" along with the original caller's phone number.

Telemarketing Guard uses the actions of our customers to identify potential telemarketing calls. The system is completely neutral to all calling telephone numbers until a report from a customer is received. As a result, all calls—telemarketing and non—will initially proceed completely unimpeded to our customers. If a customer receives an unscreened telemarketing call, it is up to them to decide whether or not to report the number, which they can do through their phone. If they choose to report the call and if a threshold of customers reporting the same number is reached, the system then begins to monitor the calling phone number and applies a number of behavioural characteristics (*e.g.,* frequency of calling, time of day concentration, sequential calling, etc.) to determine whether the call should be identified as a telemarketing call on a going forward basis.

In essence, the system promotes and relies on customer engagement to identify potential telemarketing calls. The reverse is also true. If enough customers accept a call from an identified telemarketer, the number will cease to be considered a telemarketer by the system. Several other safeguards are employed by the system to ensure that calling numbers are not erroneously identified.

Customer engagement and response has been exceptional. Based on our internal surveys, the service has increased customer satisfaction and become one of the leading reasons that customers choose to keep their phone service with Primus. In fact, few customers have selected to disable the service.

In regards to costs and implementation, the system is not overly complicated or expensive to establish and maintain. For its part, Primus currently provides Telemarketing Guard to all of its telephone customers at no extra charge. The system can also be easily grafted into an existing network and deployed, such as we did. It can work for traditional land line phones, voice-over-IP phones, or mobile phones, if the Service Provider so configures it. The service does not require customers to purchase or install any equipment or software whatsoever, nor does it require customers to actively participate in reporting in order to benefit from the reports of other customers. Additionally, the service itself can be adapted and configured to

address specific needs of customers, telephone service providers or legislative and regulatory bodies.

In addition to being a powerful consumer tool, we believe that Telemarketing Guard is consistent with the competitive interest of telecommunications carriers to provide valuable services to customers. Primus therefore welcomes the effort of the Subcommittee to identify for consumers a way that they can be equipped with the means to address unsolicited calls and to encourage carriers to offer services that provide such tools to customers.

Thank you and I look forward to any questions that you may have.

Senator MCCASKILL. Thank you very much. We appreciate you being here.

Mr. Foss?

STATEMENT OF AARON FOSS, FREELANCE SOFTWARE DEVELOPER, NOMOROBO

Mr. FOSS. Thank you, Chairman McCaskill, Ranking Member Heller, and Senator Pryor. I appreciate this opportunity to testify.

And I am here today to illustrate that the technology exists right now to block these illegal robocalls. And while there are some challenges, such as caller ID spoofing and privacy concerns, there are also effective solutions.

And to that end, there are three main points that I want to discuss. First, I am going to talk about my winning FTC Robocall Challenge entry. Then I will discuss some issues and concerns that are involved with blocking robocalls. And, finally, I am going to discuss the commercial viability of robocall-blocking services.

So, currently, the Do Not Call Registry is almost completely ineffective against these illegal mass-dialed robocallers. So to fight back, the FTC launched a competition to find new and creative solutions to this problem. They chose my proposal, which I call Nomorobo, as one of the co-winners. And that is a little play on "no mo'" robocalls.

So in real-time—well, here is how——

Senator MCCASKILL. Even we got that.

[Laughter.]

Mr. FOSS. Great. Just making sure. Just making sure.

[Laughter.]

Senator MCCASKILL. Just to reassure you. I know the rest of the country thinks we are idiots, but we got that. [Laughter.]

Mr. FOSS. Just making sure.

So here is how it works. In real-time, Nomorobo analyzes the incoming caller ID and the call frequency across multiple phone lines, and if it detects a robocaller, the call is automatically disconnected. And all of this happens before the consumer's phone rings.

So as each call is analyzed, a blacklist of robocallers is continually updated. And the more calls that come into the system for analysis, the better that the algorithm works.

I actually built this system using the same technology that these robocallers are using, so it scales inexpensively to handle millions of calls. And Nomorobo works on landlines, voice-over-IP, and cell phones on all of the major carriers and does not require any additional hardware or software. All that is required by the consumer is a simple, one-time setup to enable a free feature that is already built into the switches called "simultaneous ring."

But, as with all new ideas, there is always some skepticism. Industry players have expressed three major concerns about robocall blocking: spoofing caller ID; violating consumer privacy; and allowing legal robocalls.

So it is incredibly easy to spoof caller ID to show any phone number, and almost all of the robocallers do that. But while you can falsify the calling number, you can't falsify the calling patterns. So it is a red flag, for example, when the same number, whether it is spoofed or not, has made 5,000 calls to different numbers in the past hour. And it is also a red flag when the same number is sequentially calling large blocks of phone numbers. Both of these scenarios indicate robocalling patterns.

And so a static blacklist of known robocallers would only work in a very limited amount of situations. But by combining the caller ID, whether it is real or faked, with real-time calling pattern analysis, robocalls can effectively be detected.

And, also, with solutions like these that only look at the metadata of a call, there is no need to monitor or listen in to the phone calls, thus assuring customer privacy. The caller ID data, along with the date and time, across many phone lines, gives enough of a fingerprint to detect robocallers without having to analyze the actual content of the call.

And the final concern that has been raised is how to allow legal robocalls, such as schools and emergency notifications, to bypass robocall blocking. And this can be accomplished by building a trusted, real-time whitelist. I have already had the opportunity to speak with some of the legal robocallers, and they are very open to working on a solution that allows them to successfully deliver their calls. They want these illegal robocallers put out of business as much as the consumer does.

As my final point, I would like to show that there is proof of consumer demand for this type of service, as well as commercial viability. After I won the competition, I commissioned a nationwide survey that indicated that 57 percent of respondents would use a robocall-blocking service. And, further, 17 percent said that they would pay a monthly fee for such a service.

Since the beginning of April, when the FTC announced the winner of the competition, over 3,600 people have signed up on the Nomorobo mailing list. I have received over 400 e-mails asking, or, rather, begging, for me to release this service.

And based on the feedback that I have received, robocalls are a serious quality-of-life issue, as many people on this panel have said. I have to agree; I hear time and time again how consumers feel helpless to stop robocalls. And I think it hits at a certain core level, and we have mentioned this, but they are in their homes, with their family, enjoying their time, and they are being interrupted by a fraudster who is trying to sell them something that they don't want or they don't need.

So, members of this committee, I hope I have effectively demonstrated that the technology to defeat these robocalls exists today. It can be implemented quickly and easily with no changes to the current infrastructure. And while there are some concerns, such as spoofing and privacy, there are also solutions. The market is large

and the problem is so irritating that consumers have shown a willingness to pay for a solution.

So I thank you for your time, and I am committed to supporting your efforts in any way that I can.

[The prepared statement of Mr. Foss follows:]

PREPARED STATEMENT OF AARON FOSS, FREELANCE SOFTWARE DEVELOPER, NOMOROBO

Thank you, Senator McCaskill, Mr. Chairman, and distinguished members of the Committee. I appreciate this opportunity to testify.

I am here today to illustrate that the technology exists, right now, to block illegal robocalls. And, while there are some challenges, such as Caller ID spoofing and privacy concerns, there also are effective solutions.

To that end, there are three main points that I will discuss.

First, I am going to talk about my winning FTC Robocall Challenge entry. Then I will discuss some issues and concerns involved with blocking robocalls. And finally, I will discuss the commercial viability of robocall blocking services.

Currently, the Do-Not-Call registry is almost completely ineffective against illegal, mass dialed, robocallers. To fight back, the FTC launched a competition to find new and creative solutions to this problem. They chose my proposal, which I call "Nomorobo," as the co-winner.

In real-time, Nomorobo analyzes the incoming Caller ID and call frequency, across multiple phone lines. If it detects a robocaller, the call is automatically disconnected. All of this happens before the consumer's phone rings.

As each call is analyzed, a blacklist of robocallers is continually updated. The system is actually built using the same technology that the robocallers are using, allowing it to scale, inexpensively, to handle millions of calls. The more calls that come into the system for analysis, the better the algorithm works.

Nomorobo works on land lines, voice-over-IP and cell phones on all of the major carriers and does not require any additional hardware or software. All that is required by the consumer is a simple, one-time setup, enabling a free feature called simultaneous ring.

But, as with all new ideas, there's always some skepticism. Industry players have expressed three major concerns about robocall blocking: (1) spoofing Caller ID; (2) violating consumer privacy; and (3) allowing legal robocalls.

It is incredibly easy to spoof the Caller ID to show any phone number—and almost all of the robocallers do this. But, while you can falsify the calling number, you cannot falsify calling patterns. It is a red flag, for example, when the same phone number, spoofed or not, has made 5,000 calls to different numbers in the past hour. It is also a red flag when the same phone number is sequentially calling large blocks of phone numbers. Both of these scenarios indicate robocalling patterns.

A static blacklist of known robocallers only works in very limited situations. But, by combining the Caller ID, whether real or faked, with real-time calling pattern analysis, robocalls can be effectively detected.

Also, with solutions that only look at the metadata of a call, there is no need to monitor or listen to the phone call, assuring consumer privacy. The Caller ID data, along with the date and time, across many phone lines, gives enough of a fingerprint to detect robocallers without having to analyze the actual content of the call.

The final concern that has been raised is how to allow legal robocalls, such as schools and emergency notifications, to bypass robocall blocking. This can be accomplished by building a trusted, real-time whitelist. I have had the opportunity to speak with some of the legal robocalling companies and they are very open to working on a solution that allows them to successfully deliver their calls. They want the illegal robocallers put out of business as much as the average consumer does.

As my final point, I will show proof of consumer demand for this type of service as well as commercial viability. I commissioned a nationwide survey that indicated that 57 percent of respondents would use a robocall blocking service. Further, 17 percent said they would pay a monthly fee for such a service.

Since the beginning of April, when the FTC announced the winner of the competition, over 3,600 people have signed up on the Nomorobo mailing list. I have received over 400 hundred e-mails asking, or rather, begging for this service to be released.

Based on the feedback that I have received, robocalls are a serious quality-of-life issue. I hear time and time again how consumers feel helpless to stop robocalls. It hits at a certain core level. Here they are, in their homes, with their family, and

they are being interrupted by a fraudster trying to sell them something they do not want or need.

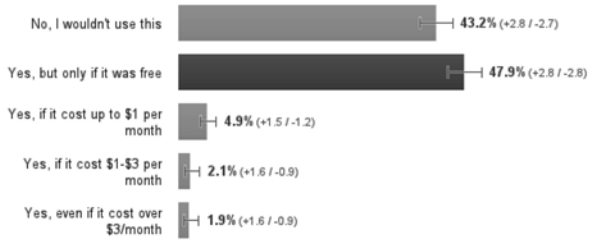
Members of this Committee, I hope that I have effectively demonstrated that the technology to defeat robocalls exists today. It can be implemented quickly and easily with no changes to the current telephone infrastructure. And, while there are some concerns, such as spoofing and privacy, there are also solutions. Stopping robocalls would be a huge win for the consumer. The market is large and the problem is so irritating that consumers have even shown a willingness to pay for a solution.

I thank you for your time and I am committed to supporting your efforts in any way that I can.

SINGLE ANSWER

Would you use a service that prevents robocalls & telemarketers from calling your phone?

Results for respondents with demographics. Weighted by Age, Gender, Region. (1379 responses)
Winner statistically significant.



	All (1379)
No, I wouldn't use this	43.2% (+2.8 / -2.7)
Yes, but only if it was free	47.9% (+2.8 / -2.8)
Yes, if it cost up to $1 per month	4.9% (+1.5 / -1.2)
Yes, if it cost $1-$3 per month	2.1% (+1.6 / -0.9)
Yes, even if it cost over $3/month	1.9% (+1.6 / -0.9)

Methodology: Conducted by Google Consumer Surveys, April 12, 2013 - April 15, 2013 and based on 1379 online responses. Sample: National adult Internet population.

Source:
http://www.google.com/insights/consumersurveys/view?survey=awabk4sgralgw&question=1&filter=&rw=1

Senator MCCASKILL. I appreciate you being here very much.

And let me just say, Mr. Stein, I was fascinated with—because you have now had experience doing this for years, and it has worked commercially for your carrier.

Mr. STEIN. Absolutely.

Senator MCCASKILL. And so let me just say for the record that the first company that is smart enough to do this in the United States, I am switching carriers to that one.

[Laughter.]

Mr. STEIN. Fair enough.

Senator MCCASKILL. And I think that the American—and I would like, Mr. Altschul, for you to address this, and Mr. Rupy.

I don't understand. We have heard from two good witnesses that the technology is available. And I understand fear of the consequences and Mencken's quote and that for every action we have in Congress, there is a reaction. On the other hand, if you look at the fears, to me, they are much less than what the reality is now that people are dealing with.

So why is it that Mr. Foss's technology is not quickly being adapted in these commercial markets? And why is it that Mr. Stein's patented product has not been licensed to an American carrier?

Mr. ALTSCHUL. I don't know about the license issues, but we do have concerns about overreaching and blocking legitimate calls.

As senators, I am sure you are more familiar than you would like to be with the kind of informational robocalls and text messages you receive from airlines when flights are delayed because of weather or other events. The volume of these calls are unpredictable, and they will flood carrier networks with identical recorded messages and text messages.

And they will carry a caller ID. That caller ID, if it is put on a whitelist, can then be spoofed, as I think we all agree how easy it is to spoof a number, and have the same fingerprint or pattern as other messages.

One of the things——

Senator MCCASKILL. Well, how does Mr. Stein's licensed product—I hate to interrupt you, but if I could get a conversation between the two of you.

Mr. ALTSCHUL. Sure.

Senator MCCASKILL. Mr. Stein, address the airlines calling with information that a flight has been delayed.

Mr. STEIN. Well, first——

Senator MCCASKILL. In reality, how does that work——

Mr. STEIN. Sure.

Senator MCCASKILL.—with your technology?

Mr. STEIN. Sure. Remember that the technology has been deployed for a number of years, so I will speak specifically to the Canadian calling patterns, which, for the record, I don't have any reason to believe are any different than American.

The reality is that the system, the Telemarketing Guard system itself, will only begin to monitor and, therefore, take action once there are reports by enough people that say, this is an unwanted telemarketer.

Further, once that call comes in, the system will not block that call. Being a carrier ourselves, we have always viewed it as our responsibility to put the two people on the phone, not impede that. But it is to give a moment of pause and to get the other party, the calling party, to press "1," record their name, and so forth.

In the event of delayed flights and things like that, these things tend to go right through. There hasn't been any effect. We have never seen a complaint like that because——

Senator MCCASKILL. So no consumer is going——

Mr. STEIN.—people have never——

Senator MCCASKILL.—to call——

Mr. STEIN. That is right. No consumer——

Senator MCCASKILL. Nobody is going to call and say, the airline let me know my flight was late. And that is what the initial——

Mr. STEIN. That is right.

Senator MCCASKILL. That is the initial beginning of the block, is a critical mass of people calling and saying, hey, these guys are——

Mr. STEIN. That is right, because they——

Senator MCCASKILL.—rip-off people or they are trying to sell me siding.

Mr. STEIN.—they are not objecting. The consumer is not objecting. And I talk about this benefit, in that nobody other than the consumers themselves decide what is and what is not an unwanted telemarketer or robocall. And so that——

Mr. ALTSCHUL. But my point is that that number, which is welcome and legitimate and properly described on caller ID, is basically the identifier that the carrier and the customer and Mr. Stein's system has to track wanted and unwanted calls.

Right now, there is no need for scammers to actually pick numbers that consumers would recognize as the source of messages, informational messages, they would like to receive. But there is no limitation on a fraudster's ability to use an airline's number to fill out the caller ID field in the robocalls and messages that they send.

Senator MCCASKILL. Well, let me just address that. So let's assume in Canada, since 2007, that a fraudster got a hold of United Airlines' number and started using that.

How would it work with your system, Mr. Stein, if that happened, if they spoofed a legitimate number that no consumer would complain about, but they started using it and——

Mr. STEIN. Right.

Senator MCCASKILL. What would happen? How would that work?

Mr. STEIN. Two quick comments.

First, the system is quite smart. And over the years that we have tuned it and built and enhanced it, we have built in a great many safeguards to prevent this exact thing from happening. And I won't elaborate in full detail on all those, but such is to say that if such a thing were to happen and reports were to start to come in, one would assume that at the same time the airline is using that phone number, too, and therefore a lot of those calls are getting accepted by our customers.

So we would be seeing votes going in both directions, and the system becomes increasingly skeptical and looks for what distinguishes the two types of calls, and then is able to break them down based on many of the other criteria that are no longer using just, say, the caller ID, which is the thing that is easy to spoof. There are a lot of other characteristics in a phone network that are available that we use.

Senator MCCASKILL. He wins.

Mr. ALTSCHUL. Well, give me another chance.

[Laughter.]

Mr. STEIN. I would be happy to——

Mr. ALTSCHUL. As Mr. Foss testified, his technology is the same technology or built on the same roots as the technology these scammers are using. And what we have found, particularly in the area of policing text messages that come across carriers' gateways from the Internet is, as the carriers become more sophisticated in

looking at the fingerprints, looking at the volume of calls, the number, the speed, the number of identical messages, the fraudsters become increasingly better educated and sophisticated at the same time.

So this is a cat-and-mouse game. You set a threshold, say, originally of 10,000 messages a minute or an hour, and any message volume for identical messages above that would get caught. Before long, the fraudsters set their threshold at 9,000 messages. You lower the threshold again, the fraudsters find out their messages aren't going through, they change their threshold to still stay under the limit. The costs of doing this really are almost zero.

And so, for every action and every, you know, time you raise the wall, the bad guys come back at you with a taller ladder.

Senator MCCASKILL. Well, I think the point that is being made, and for Mr. Rupy and Mr. Altschul, the point that is being made is we have the capability of being as sophisticated in terms of technology as the bad guys. And there are a number of different algorithms that could be used to identify the bad guys that currently our American carriers just aren't bothering to use.

And that is hard for me—I mean, Mr. Foss is on the precipice of hopefully rolling out a product that will show that Canada won't be a decade ahead of us, as opposed to merely—what are we up to now? Six, 7 years? You know, if the sky was going to fall, I think Mr. Stein probably wouldn't be here.

And, Mr. Rupy, I will wait for Mr. Heller to ask questions to come back and ask your take on this.

Because it worries me that we are going to say, well, you know, if we do this to try to catch the bad guys, they are just going to do something else. Can you imagine the amount of money we could have saved if we just would have just given up on trying to interdict drugs?

Mr. ALTSCHUL. Well, and to be clear——

Senator MCCASKILL. "Well, if we do that, if we go after their airplanes, they are going to do boats. Let's not do the airplanes. Or if we do boats, they are going to go over, you know, the Mexican border. Let's don't do that, because then they will just go over the Mexican border."

We just keep trying. And I think this is one of these issues that we really haven't teed up yet to really try hard.

Mr. ALTSCHUL. Well, to be clear, wireless carriers, with respect to SMS text messages, are doing exactly what you have described, and it has been an iterative learning experience. And some of the lessons learned—it is just basically a spam filter, but a spam filter for text messages—are instructional as to how smart the bad guys are.

Senator MCCASKILL. We are smart.

Senator Heller?

Senator HELLER. Madam Chairwoman, thank you.

Mr. Stein, I want to talk a little bit about Telemarketing Guard. Is that a unique system in Canada?

Mr. STEIN. Yes.

Senator HELLER. Are there any other carriers that have anything that is similar to what you have?

Mr. STEIN. No. We—no.

Senator HELLER. You talked about years. How long has it taken you to develop this particular system?

Mr. STEIN. We came up with the idea in early 2006. We had it commercially deployed, built, tested, et cetera, commercially deployed by, I believe, early 2007.

Senator HELLER. Any initial weaknesses to the system, things that——

Mr. STEIN. No, I wouldn't say there were weaknesses. I would say we learned lots in the initial days, but nothing concerning, no.

Senator HELLER. OK.

Mr. STEIN. No complaints from customers, et cetera, nothing like that.

Senator HELLER. Have you been approached by any other carriers, whether in Canada or the U.S., to borrow or buy the technology?

Mr. STEIN. A little bit. We participated in the FTC's robocall summit in the fall last year. After that, we had a couple of calls, some light inquiries, but nothing pursued too greatly.

Senator HELLER. So you got beaten out by Nomorobo?

[Laughter.]

Mr. STEIN. Well, in fairness, we didn't submit Telemarketing Guard to the challenge, as we were not eligible for it. We had presented at the summit that preceded the challenge.

Senator HELLER. OK. Are you aware of any barriers that may prohibit bringing this kind of technology from Canada to the United States?

Mr. STEIN. No, I am not.

Senator HELLER. OK. OK.

Mr. Foss, congratulations.

Mr. FOSS. Thank you.

Senator HELLER. And you said you had about 3,600 people now that have—do they buy your product, they download your product? What do they do? How does someone know to get involved in what the FTC has produced in this case?

Mr. FOSS. Sure. And that is the funny part, is that it is not even available yet. It was just the announcement. I set up a website, I put in my e-mail and said, it is coming soon. Thirty-six hundred people said, give this to me, whatever it is. They don't know how much it is going to be, how it is going to work. They just know that there is a problem. So this is just basically the press that has been generated by this and directed them to the website.

Senator HELLER. When do you think it will be readily available?

Mr. FOSS. By the end of the summer, actually.

Senator HELLER. So you will have some kind of a program to make sure that the American public are aware of what your product is?

Mr. FOSS. Exactly, exactly. After the competition, I wound up talking to a bunch of investors. I got enough seed money to go and build this into a beta to actually go and launch it and to address some of these exact concerns to see—you know, the best way is just to prove that it will work.

And one of the things, I think, that Mr. Stein's product is actually better at than mine, because he is a carrier, is the worst-case scenario, I think, in Mr. Stein's case is that the call gets diverted

to voice-mail. You know, a lot of these things—the thinking that went into it before everybody had voice-mail was that, and especially on mine, is that the call is going to be disconnected, you are going to lose the call forever. But now if we can just divert it to voice-mail, much like spam does into your spam filter, I think everybody would rather have a voice-mail box with five or six robocalls than five or six robocalls.

Senator HELLER. OK.

You mentioned during your testimony that there were some industry players that were concerned with this technology. What are those concerns, and what have you done to address those concerns?

Mr. FOSS. Yes. So the main concern is the caller ID spoofing. A lot of players feel and what they say is that, well, the caller ID is always going to be wrong, so therefore we can't stop this problem.

But, again, I see it a little bit differently. And by using the caller ID, whether it is real or not, with these calling patterns, real-time calling patterns, that we can actually start—again, even if it is faked, it doesn't really matter.

The second is the consumer privacy. A lot of people have said that this isn't like e-mail, because in an e-mail you can go and analyze the content, and that in order to do this, you would have to listen in on everybody's phone calls.

And I don't believe that is correct. I think that using this caller ID, with the calling patterns—and, again, much like the other solutions that are here—some other reported data, the FTC data, you actually have a stab at making this—it is not going to be perfect.

It is absolutely not going to be 100 percent. But even with spam filters today, certain spam gets through, sometimes real e-mails get into your spam folder. And I think that we need to try it, and I think that we need to start somewhere.

Senator HELLER. Mr. Rupy, you said in your testimony that technology is constantly changing. Do you believe a solution like this, Nomorobo, is a solution that can work?

Mr. RUPY. Senator, that is a fantastic question, and I have to say I think it is absolutely fantastic that there are innovators like Mr. Foss out there who are working to develop these various solutions. And as Mr. Foss acknowledges, there are challenges to some of these technological solutions.

And my point on the technological issue is that, like so many issues that arise in this Internet space, it is a constantly evolving and moving target. So I think in terms of designing a single technological silver bullet that can fully address the robocall issue, that will be an ongoing challenge.

Senator HELLER. One more question, if you don't mind.

Senator MCCASKILL. Sure. Take all the time you would like.

Senator HELLER. Mr. Altschul, government agencies cited their number of complaints. Do you find those numbers to be accurate?

Mr. ALTSCHUL. Carriers receive complaints. The government agencies at all levels, Federal and state, receive these complaints. So they are accurate, but our gripe is the way they are actually displayed and recorded by the Federal Communications Commission. They are divided across services, and it really doesn't provide a clear picture of what is going on or the magnitude of the problem.

Senator HELLER. Has the industry had an opportunity to verify the number of cites and complaints that——

Mr. ALTSCHUL. I am not in any way challenging the numbers. It is how they are reported.

Senator HELLER. OK.

Thank you.

Senator MCCASKILL. Mr. Rupy, when the common carriers see mass amounts of calling and short calls in a massive quantity come over the transom, what do you do?

Mr. RUPY. Senator, that is where, during my oral testimony and the written testimony, several of our member companies have these network operations centers. And there are measures that these companies can take to address these mass-calling events. And that is where some of these working groups that I mentioned come in.

Our experience——

Senator MCCASKILL. What do they do now, though? You said they take different measures. Can you give me an example of one of the—you know, you don't have to name the carrier, but give me an example of—let's assume one of my carriers, which is AT&T, let's assume a massive amount comes over in a short period of time in a geographically concentric area. Do you know what they actually do when that happens, if anything?

Mr. RUPY. Senator, I know they take actions. I don't know what those specific actions are. And we would be happy to provide that information.

Senator MCCASKILL. I think that would be important for us to know.

Mr. RUPY. Absolutely. Sure. And——

Senator MCCASKILL. Go ahead.

Mr. RUPY. And just to keep in mind, oftentimes these mass-calling events, I mean, they are not all directly attributable to robocalling events. So, you know, for example, on September 11th, we had mass-calling events in New York City and Washington, D.C. So——

Senator MCCASKILL. Well, I think that is pretty obvious, though. I mean, obviously everyone understands that.

I am talking about, all of a sudden it is Kansas City—and, you know, it is interesting. I was on a radio program this morning talking about this. And they had gone out and done a man-on-the-street interviewing people. And every single person they talked to said they had gotten a call about siding. So, clearly, there had been a massive amount of calling in the Kansas City area about siding.

And that is what I am talking about. I mean, there is nothing going on, there is no extraordinary weather event. You know, if a plane is late, we are talking about maybe 100, 200 people; we are not talking about thousands.

I need to know what, if anything, these carriers are doing. And do they feel an obligation to do something?

Mr. RUPY. Well, and they are certainly taking action on those issues, Senator. But I think one of the points that was raised earlier by various folks on the panel here is that, under our current legal framework, regardless of whether it is a mass-calling event or sort of a standard calling volume, we are under a legal obligation to complete those phone calls and——

Senator MCCASKILL. Well, so you are saying that you legally couldn't adopt Mr. Stein's technology?

Mr. RUPY. As I understand——

Senator MCCASKILL. It connects; it just decides whether it goes to voice-mail.

Mr. RUPY. As I understand Mr. Stein's and Mr. Foss's technology, to a certain degree you have these—the decision is removed, to a certain degree, from the consumer and is made by the carrier with——

Senator MCCASKILL. No, that is not true. That is not true. I don't think that is true.

Mr. Stein, the carrier is not making the decision, is it?

Mr. STEIN. No, the carrier does not make that decision. I can only speak, of course, to our system.

The system doesn't block a call under any circumstance, other than if the customer were to say, here is one given number that I don't want, a blacklist, available on many services.

In the case of Telemarketing Guard, it impedes the call and asks the caller to press a digit to record their name. But in all of those cases, those recorded names, the phone call is made, et cetera.

And I am not a lawyer, so I can't speak to the legality of it. I am sure we have a lot of them in the room, though.

[Laughter.]

Senator MCCASKILL. I would really appreciate, Mr. Rupy, if you would take back to the legal staff at your organization the specifics of both Mr. Stein's and Mr. Foss's technology and get back to us with what specific problems, from a legal framework, you believe that there are.

I think if this were offered by a carrier, you know, I am just shaking my head that an American carrier has not tried to adopt one of these technologies because I think it is such a winner in an open, capitalistic, competitive market. And by my television ads that I watch, all the carriers are pretty darn competitive right now. I mean, they are desperately not just trying to get new customers; they are trying to hold on to customers. Because, you know, now that we can take our phone numbers, there is this incredible desire to see if you can't get somebody to walk from someone else to you.

And for the life of me, I can't figure out why you all are not more aggressively going after this very desirable technology on behalf of consumers.

Mr. RUPY. Senator, we can absolutely provide that information.

And just to be clear, I mean, our member companies do offer—and I always encourage consumers to reach out to their respective carriers to see the services that they are offering. And they do range from things like, whether it is caller identification, to conditional call forwarding, to anonymous-call blocking. There are tools that the carriers are providing and continuing to develop.

And, again, we operate under that very stringent obligation to complete those calls. And it is very clear to us that that is something we need to comply with.

Senator MCCASKILL. Well, I don't want anybody to break the law.

[Laughter.]

Senator MCCASKILL. But I have a feeling we can do this with the technology that is out there without breaking any law and maybe

even without us having to write any laws. And wouldn't that be special? Because it is always nice when we can reach a marketplace solution in the private sector.

And I know that I am getting a nodding head from Senator Heller right now.

[Laughter.]

Senator MCCASKILL. It is always better to do it in the marketplace with a competitive solution as it relates to capitalism than it is for the government to come in with a heavy hand and try to impose a solution.

So I think it is pretty important that we hear from you about what you see the legal missteps would be, since we have an example of technology that has been used in a country that also embraces capitalism——

[Laughter.]

Senator MCCASKILL.—and it seems to be working and working well for their company. So I would really appreciate you all with that follow-up.

Do you have any other questions?

Senator HELLER. Yes, I do. And thank you, Madam Chairwoman, and thanks for your comments and to follow up.

And this is for the panel. I guess the bottom line with this particular hearing is, should the FTC and the FCC be given enforcement powers or additional enforcement powers, or can this be solved through the private industry itself?

Mr. Rupy?

Mr. RUPY. Senator, I think as Senator McCaskill mentioned earlier this morning, the existing legal framework dealing with robocalls appropriately targets the bad actors who are engaging in this fraudulent activity.

And I think to the extent that we continue to target that enforcement and make that enforcement aggressive against those actors, that is the ideal solution here. Because, as I have said in my written testimony, our member companies work with agencies like the FTC to prosecute these actors. We want to catch them as much as everyone here in this room.

Mr. ALTSCHUL. I would agree. I think it requires a holistic solution. Everybody has to play a role. And, certainly, the enforcement agencies have a critical role, as do consumers, as does the industry.

One of the things that our industry has begun looking at, which is far from yielding any results, is how to better map and trace these calls and messages when they cross through the Internet to traditional carrier networks.

As you may know, carrier networks, when they were closed, used a signaling system called Signaling System 7—there never was a System 8—as a way of setting up and identifying calls for billing, tracing, all kinds of things. The Internet uses a system call SIP, Session Initiation Protocol. And mapping or being able to marry these two very, very different kinds of protocols is part of the problem right now the enforcement agencies and everyone is having in trying to trace this back to the source of these messages.

And if the technical experts who have begun to work on this marrying of SIP to SS7 messaging protocols are able to solve that

problem, we will enable, you know, great progress in identifying and stopping these messages at the source.

Senator HELLER. I am going to guess Mr. Stein and Mr. Foss believe that there is a private-sector solution to these problems, and I will leave it at that.

I just want to ask one more question for you, Mr. Rupy and Mr. Altschul: if you have any response to the FTC raising the issue of abolishing the common carrier exemption. Do you have any feel on that?

Mr. RUPY. In terms of the common carrier exemption, Senator, I think, as Senator McCaskill raised in her testimony this morning, we have these issues where we have sort of conflicting regulations, one for wireline, one for wireless. And I think to the extent you start expanding the scope of, you know, numerous agencies regulating similar players in the field, that gets to be problematic.

Second, we fully support—and what I thought I heard in the earlier testimony from the FTC is that, to the extent there is an entity out there engaging in illegal activity, they are going to go after that entity, as well they should. And we fully support that, whether they are a common carrier or whomever.

Mr. ALTSCHUL. As the FCC's Mr. Bash testified, there is an existing working relationship between the two agencies. They are both enforcing the same laws. And I think that there are some institutional advantages that each institution has developed in their respective areas. I am not aware that it is a problem that has actually deterred any kind of investigation or enforcement activity.

Senator HELLER. OK.

I want to thank the witnesses for your time and energy.

And, Madam Chairwoman, thank you for holding this hearing.

Senator MCCASKILL. I appreciate everyone being here.

I will tell you that I know that there are concerns, and all of the concerns about what can be done are based in wanting to follow the law and stay true to what your mission is as carriers, whether it be wireless or wired.

I do want you to know that I am going to follow up in 3 months and ask to find out what your members are doing in this regard and what they feel like they can do. And whatever information that you can give us in the next 3 months that would spell out the problems you would have with adopting either the technology that Mr. Foss is ready to roll out by the end of the summer—do you know what it is going to cost, Mr. Foss?

Mr. FOSS. I am actually hoping to offer it for free.

Senator MCCASKILL. OK. So am I going to have to look at ads?

Mr. FOSS. No, actually, because I figure that on the——

Senator MCCASKILL. How are you going to do that? We know we have to look at ads if it is free.

Mr. FOSS. I didn't put this in my testimony, but this problem doesn't only affect the consumer; it affects businesses.

Senator MCCASKILL. Right.

Mr. FOSS. And as the other panel talked about it, the PSAPs, the emergency call centers. The FCC put me in touch with the organization that manages a lot of these 911 centers. I think there are over 5,000 of them. You know, this do-not-call list is being implemented.

And, you know, I said to them, I said, if there was a blacklist, a real-time blacklist, an up-to-date list of the numbers that you shouldn't be answering, would that be helpful? And they said that they had never even thought about that, and if that existed, it would be amazing.

So I think that there is an actual, you know, this data set of the real-time robocallers and the calls that you shouldn't pick up on, even I think on the consumer side—or, I am sorry, on the business side or anybody who has large call centers, you know, thousands of phone lines.

And I spoke to some that are in financial services, you know, the Citibanks and the Chases of the world. Every call that comes in, they have to go and screen for fraudsters. So if they know before they even send it for screening that they should immediately dump it, I think that there is a real valuable asset there.

So I think that by doing it with the consumers and offering them, you know, a really good service of blocking the robocalls, my thesis is that I can make money on the business side.

Senator MCCASKILL. On the business side.

Mr. FOSS. Yes.

Senator MCCASKILL. OK. Well, you don't need to worry; when you roll out, I will give it a try.

Mr. FOSS. Sounds good. Thank you.

Senator MCCASKILL. And thank you, Mr. Stein, for coming from Canada. And we will look forward to following up with our carriers here in America to see if we can't reach a solution.

Because I do know this: With the technology that is available, if it is just about chasing these guys, law-enforcement-wise, around the country, we are never going to get the results that consumers deserve on this.

So I thank you all very much for being here. We appreciate it.

[Whereupon, at 11:39 a.m., the hearing was adjourned.]

A P P E N D I X

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. CLAIRE MCCASKILL TO LOIS GREISMAN

Question 1. Ms. Greisman, the FTC has essentially placed a call for help with robocalls. Then-FTC Chairman Jon Leibowitz noted last year at a summit on the issue, "Law enforcement alone can't stop the robocalls." No matter how many cases the FTC brings, the agency says there is not much more it can do from an enforcement perspective to abolish illegal robocalls. As a result, the Commission held a public competition to find a viable technological solution that could provide some level of defense against robocalls. Why do you think a technological solution is the best answer to this problem?

Answer. I do not believe there is one best answer to this problem; rather, the FTC must simultaneously pursue multiple strategies to fight illegal robocalls. We launched the Robocall Challenge because technological advances caused the explosion in illegal robocalls, and we believe it is important to encourage technological solutions that can counteract the proliferation of illegal robocalls. But the agency's other efforts—including law enforcement, coordination with experts, and consumer education—continue.

As one example, we continue our aggressive and strategic law enforcement, and the actions we have brought in Federal court have shut down entities responsible for *billions* of illegal robocalls. For instance, the FTC put a robocall operation out of the telemarketing business and recovered approximately $3 million under a settlement resolving FTC charges that the defendants bombarded consumers with more than two billion robocalls, including the ubiquitous "Rachel from cardholder services" calls, sometimes using false Caller ID names, such as "SALES DEPT." *See FTC* v. *Asia Pacific Telecom, Inc.,* available at *http://www.ftc.gov/opa/2012/03/asiapacific.shtm.*

Question 2. The FTC selected three winners in its robocall challenge. Why were those three entrants chosen as winners? What about their submissions, compared to the rest, does the FTC believe will best limit fraudulent robocalls for America's consumers?

Answer. The Robocall Challenge submissions were judged by Steve Bellovin (Chief Technologist from the FTC), Henning Schulzrinne (Chief Technology Officer at the Federal Communications Commission), and Kara Swisher (co-Executive Editor of *All Things Digital*). The judges reviewed hundreds of entries to find submissions that best met all three of the judging criteria: (1) Does it work?; (2) Is it easy to use?; and (3) Can it be rolled out? What follows is a more detailed explanation of the criteria, which was publicly posted at *http://robocall.challenge.gov/details/criteria:*

Does it work? (weighted at 50 percent)

- How successful is the proposed solution likely to be in blocking illegal robocalls? Will it block wanted calls? An ideal solution blocks all illegal robocalls and no calls that are legally permitted. (For example, automated calls by political parties, charities, and health care providers, as well as reverse 911 calls, are not illegal robocalls.)
- How many consumer phones can be protected? What types of phones? Mobile phones? Traditional wired lines? Voice over Internet Protocol ("VoIP") land lines? Proposals that will work for all phones will be more heavily weighted.
- What evidence do you already have to support your idea? Running code? Experiments? Peer-reviewed publications?
- How easy might it be for robocallers to adapt and counter your scheme? How flexible is your scheme to adapt to new calling techniques? How have you validated these points? Remember that the real test of a security system is not whether or not you can break it; it's whether or not other people can.

Is it easy to use? (weighted at 25 percent)

- How difficult would it be for a consumer to learn to use your solution?
- How efficient would it be to use your solution, from a consumer's perspective?
- Are there mistakes consumers might make in using your solution, and how severe would they be?
- How satisfying would it be to use your solution?
- Would your solution be accessible to people with disabilities?

Can it be rolled out? (weighted at 25 percent)

- What has to be changed for your idea to work? Can it function in today's marketplace? (E.g., Does it require changes to all phone switches world-wide, and require active cooperation by all of the world's phone companies and VoIP gateways, or can it work with limited adoption?) Solutions that are deployable at once will be more heavily weighted, as will solutions that give immediate benefits with even small-scale deployment.
- Is deployment economically realistic?
- How rapidly can your idea be put into production?

The judges selected the winners from among the contestants' many informed, creative, and intelligent submissions, based on the criteria laid out above.

While I cannot speak for the judges, I believe the winning solutions contain promising ideas about how to address difficult realities such as the limitations of the telecommunications infrastructure and the prevalence of caller ID spoofing. For example, one of the winners, Aaron Foss, proposed an innovative method of deploying a filter, via a cloud-based service that consumers could access using a simultaneous ring feature on their current telephones. The other two winners tackled the problem of caller ID spoofing in novel ways; they each designed their own mechanisms that can help determine whether an incoming call's caller ID information is authentic or not. I believe the three winning solutions represent real breakthroughs compared with what is currently available in the marketplace.

Question 3. The United States Telecom Association, at the hearing, said its member companies work with various law enforcement agencies, including the FTC, to prosecute individuals and entities responsible for fraudulent robocalls. Would this be an accurate assessment of the industry from the FTC's point of view?

Answer. Many of the members of the United States Telecom Association do assist us with investigations of those responsible for illegal robocalls, and we greatly appreciate this assistance. As I stated in my testimony, I do believe that carriers could be more proactive in identifying suspicious activities on their networks that could be indicative of illegal robocalling.

Question 4. What percent of the FTC's investigations into potential violations of your telemarketing and robocall rules are initiated by information voluntarily submitted by industry to your agency? Since the establishment of the National Do Not Call Registry, how many times have telecommunications providers alerted the FTC to potential violations of either your telemarketing rules or robocall rules?

Answer. Generally speaking, industry players have not proactively alerted the FTC to potential violations of our rules. The more common scenario is that our attorneys or investigators contact a carrier about a potential rule violation, and the carrier then assists us in obtaining available information about that particular call campaign.

Question 5. The FTC and the FCC have clear rules establishing what is, and what is not, allowable when it comes to robocalls, and both agencies have taken enforcement actions to stop illegal robocalls. Yet despite all of these efforts, intrusive and fraudulent robocalls have proliferated. Technological solutions may very well provide the American public with relief, but I also think that there is no substitute for strong law enforcement. As such, I am interested in learning further about the FTC's and the FCC's efforts and what more can be done to stop illegal robocalls. What are the limitations your agency faces in bringing more enforcement cases? Is there a need for legislation to assist your efforts?

Answer. We do face challenges related to law enforcement against illegal robocallers. Given automated dialing technology, inexpensive long distance calling rates, and the ability to move internationally and employ cheap labor, robocalling has become an attractive marketing channel to fraudsters. And new technologies make it easy for robocallers to hide their identities by spoofing and regularly changing caller ID information, as well as by allowing them to generate calls from any location in the world where they have access to an Internet connection. In addition, a single call now traverses the networks of many different service providers and no single entity knows the entire path of a call; the result is that every entity must

timely provide data in order for law enforcers to successfully trace a call. These factors, among others, make investigation and enforcement increasingly difficult and time-consuming.

Separate from these challenges, and as I stated in my testimony, I believe the common carrier exemption is outdated and unnecessary. The telecommunications industry has become much more complex and diversified, and the line between what is and is not a carrier has blurred significantly. Currently, numerous entities participate in delivering the robocall, including the associated caller ID information, and not all of their functions fit squarely into the categories of carrier or non-carrier. It would be far more efficient if the FTC could address illegal telemarketers and those who facilitate their activities without having to determine which of the entities that participated in a single call campaign might be considered common carriers. In other words, the exemption creates an obstacle to effective law enforcement efforts against robocallers. For these reasons and in this context, I support elimination of the common carrier exemption.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. AMY KLOBUCHAR TO LOIS GREISMAN

Question 1. I want to applaud the FTC for undertaking the "Robocall challenge" as an innovative way for government to work with the private sector and software engineers to find solutions. Ms. Greisman, can you discuss the process for the challenge and how you chose the awardees? What is the next step for the FTC in encouraging getting these products to market and helping to fight fraud?

Answer. The Robocall Challenge was the FTC's first public contest under the America COMPETES Reauthorization Act of 2010. One of our first steps involved choosing three experts to judge the challenge. Two of our judges were the Chief Technologists from the FTC and the Federal Communications Commission—Steve Bellovin and Henning Schulzrinne—who both have extensive technical backgrounds in telecommunications, Voice over Internet Protocol ("VoIP") technology, and security. The third judge was Kara Swisher, one of the co-founders of *All Things Digital* and someone who has broad expertise regarding consumer technology products and the consumer experience. The judges helped determine the judging criteria, which were: 1) Does it work? (50 percent); 2) Is it easy to use? (25 percent); and 3) Can it be rolled out? (25 percent). For more information regarding these criteria, please visit this website: *http://robocall.challenge.gov/details/criteria.*

We publicly announced the Robocall Challenge on October 18, 2012, and submissions were due by January 17, 2013. We received 798 eligible submissions. Pursuant to the official rules, an internal panel screened these submissions to determine, in accordance with the judging criteria, which submissions warranted further review by the judges. The internal panel identified 266 submissions that were then reviewed by the expert judging panel. Following numerous meetings and discussions, the judges chose seven finalists and assigned numerical scores to each. Two engineers from Google won the nonmonetary award in the large organization category. The judges found a tie within the category of individuals and small organizations; thus, the two winners split the $50,000 prize.

The goal of the challenge was to stimulate the marketplace and encourage the development of new ideas. The FTC does not take an active role in bringing the winning solutions to the market and does not endorse particular consumer products. To identify and reward the challenge winners and promote the challenge as a tool to spur innovation in the marketplace, we held a press conference and produced videos about the challenge. Through these means and related efforts, we think we have helped to encourage innovators to focus their talents on developing a technical solution to the problem of illegal robocalls.

Question 2. Ms. Greisman and Mr. Bash, we know that technology will continue to evolve. How are the FTC and the FCC working to keep up with these evolutions in communications to protect consumers from future scamming operations?

Answer. We issued the Robocall Challenge to spur technological innovations that would complement our law enforcement efforts to protect consumers from scammers. As we looked at the marketplace in the context of e-mail spam, we saw numerous experts deploying technological solutions to protect consumers against spammers and fraudsters, but relatively little focus on robocalls. Through the challenge, we sought to bring more attention to illegal robocalls and prompt rich and vital initiatives to address the problem. I believe that the challenge accomplished this goal and that the winners' sophisticated filters and other similar products can significantly enhance consumer protection. Notably, none of the four technology experts who created the winning solutions had ever worked on the robocall problem before. I will

add that while the challenge spurred nearly 800 innovators to submit proposals, it also prompted others to go to the drawing table. We have heard that the FTC's recent robocall initiatives gave other entrepreneurs new connections and ideas to fight illegal robocalls, which is an important ripple effect. We hope this will help stimulate the market to develop technology that will combat telephone spam, similar to efforts to develop technology to reduce e-mail spam.

In addition, we work to ensure that our internal team at the FTC keeps up with the ongoing evolution of communications technology. For example, we regularly speak to and work with technical experts who can help us understand evolving technology, including academics, industry insiders, and entrepreneurs. We partner with internationally renowned technological associations—such as the Messaging, Malware and Mobile Anti-Abuse Working Group and the Internet Engineering Task Force—to work toward a longer-term goal of changing the telephone network protocols to allow for authenticated telephone calls. We also use our evolving knowledge to innovate with respect to our own law enforcement investigations and targeting. As one public example, last October we announced our new robocall honeypot, which is a group of phone numbers that allows the FTC to receive robocalls directly and helps the agency gather evidence and take quick action.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MARK WARNER TO LOIS GREISMAN

Question 1. Over the past year or so, my office has seen a marked increase in calls and letters regarding possible abuses by some telemarketers. Since January 2013, my office has heard from more than 300 people requesting assistance with the Do Not Call List, and since taking office in 2009, my office has heard from over 1200 people on this issue. A small sampling of some of the concerns we have received are also included in this document for the record.*

---

* Selected Constituent Robocall Concerns

"It is an invasion of our privacy, and it ties up our phones and disrupts our lives to get as many as 15 calls every single day when we have been on the donotcall list since day 1. Anything you can do about this issue will be greatly appreciated."

—Constituent from Arlington, VA 5/26/2012

"I am registered on the "Do Not Call" list for my home phone (not cellphone) and I am still getting many solicitation "robo calls" for lower credit card rates, car warranties, and other commercial products. Some callers block caller ID. I systematically report these callers via the "report a violator" process on the Registry website. I have been on the do-not-call registry since its inception, and I have verified this on the Registry site. I also put my elderly mother's home phone number on the DNC Registry several years ago. She also gets many solicitation calls. I am well versed on the types of calls that the DNC system is supposed to address, and the kinds of calls that are excepted. I am astonished at the number of calls I am getting even as I am on the DNC list."

—Constituent from Fairfax, VA 05/04/2012

"xxx-xxx-xxxx [redacted]. This number continues to call with impunity, even though they are on my FTC Do Not Call Registry, and several other residents I'm friends with. They are scam artists, trying to mine personal information, and the FTC hasn't responded to my concerns. Are you game for going after this group of obvious scammers, because a lot of vulnerable citizens, could be prey for their scam which involves lowering debt. They call themselves [redacted], and they are a company I and others have never done business with. Thank you kindly."

—Constituent from Fairfax, VA 06/06/2012

"I have been getting calls on my home phone from a 'Credit Card Services' for over a year now. I have submitted at least five complaints on the FTC website and at least two complaints' on the 'Do Not Call' website. I have asked to speak to a supervisor numerous times, only to be hung up on. I have told them over and over and over again to not call me. I have threatened them with FTC complaints. I have received over 30 calls from this company and have turned in many complaints to the Federal Trade Commission and nothing seems to work. If you look on the internet, you will see tens of thousands of complaints. Therefore, I would like to request that you (my congressmen) get the Federal Trade Commission to do their job and shut these people down."

—Constituent from Alexandria, VA 07/23/2012

"Over the last couple of months, I've been getting an increasing number of robo-dialer/recorded commercial calls in violation of the Do-Not-Call registry. Many have been from the same 'crook', often "Credit Card Services." I've reported most of them on the FTC's Do Not Call registry. (That is not counting the growing number of political calls, which unfortunately are not violations of Do Not Call)."

—Constituent from Reston, VA 08/20/2012

"Senator—Please have someone on your staff Google (xxx)xxx-xxxx [redacted] and you will see several websites dedicated to complaints about harassing phone calls from this number asking

As a supporter of the Do Not Call Act, I sympathize with the frustration of my constituents. I recognize that the same technology that is allowing telephone service providers to more efficiently manage networks is also enabling disreputable callers to abuse the system.

Still, it seems to me that if we can't find a technical solution to abusive telemarketing calls, that raises many serious questions as well. I encourage you to think more creatively about possible solutions, and about any legislative authorities that would better enable the FTC to keep pace with technology. For instance, have similar problems occurred in other countries? If so, are there any solutions adopted in other markets that might be applicable in the U.S.?

Answer. Yes, the same problems are occurring in other countries. We have undertaken a global search for solutions, and we did identify the "Telemarketing Guard" by Primus Telecommunications Canada, whose Chief Technology Officer Matthew Stein testified on July 10 after also appearing at our Robocall Summit the previous fall. We have actively encouraged carriers and others to bring Telemarketing Guard or a similar solution to consumers in the United States. Telemarketing Guard is currently only available to approximately one million Canadian consumers.

Unfortunately, we are unaware of successful solutions that have been more broadly adopted in other countries. Instead, the FTC is actively participating in a joint search for such solutions. Our Office of International Affairs ("OIA") coordinates with our international counterparts on related issues. For example, our OIA participates in several multinational networks that coordinate on broad strategic matters related to illegal telemarketing, including through the London Action Plan ("LAP") on international spam enforcement cooperation and the Centre of Operations Linked to Telemarketing. Through our involvement in the LAP's Do Not Call Working Group, we are actively engaged with the multinational organization's initiatives to develop an international strategy related to caller ID spoofing. One example is the LAP's upcoming October meeting, which is being held in coordination with the Messaging, Malware and Mobile Anti-Abuse Working Group. The FTC, with the Canadian Radio-television and Telecommunications Commission and the Australian Communications and Media Authority, will lead a discussion of proposed solutions—technological, policy and enforcement—that can be considered for global telecommunications systems. Also at that meeting, we are leading a panel on telephony abuse, which includes caller ID spoofing.

We are also fully engaged with international communities of technical experts that are working to address this problem, such as the Internet Engineering Task Force. In addition, we have collaborated with foreign law enforcement authorities on particular cases, for example working closely with Canadian law enforcement on *FTC* v. *Direct Financial Management, Inc.,* No. 10 C 7194 (N.D. Ill. Feb. 8, 2012), and *FTC* v. *Economic Relief Technologies, LLC,* No. 1:09–cv–03347 (N.D. Ga. Jul. 22, 2010).

Question 2. In 2012, the Federal Trade Commission (FTC) challenged innovators to come up with a solution that would block illegal commercial robocalls on landlines and mobile phones. One of the proposed solutions creates a filtering system, similar to an e-mail spam filter, that intercepts and filters out illegal robocalls using a technology that "blacklists" and "whitelists" phone numbers. The proposal envisions a consumer-facing system, however, others have suggested that a network-based system might be more efficient and less burdensome for consumers.

Do you believe that a filtering system would be effective? If so, do you believe it should be implemented by networks or by consumers? If not, do you have ideas for a better solution?

Answer. I believe effective solutions for blocking illegal robocalls could be based on any number of possible technical approaches. An effective solution might, for example, be based on filtering, and could be designed to be implemented by networks, consumers, or otherwise. However, it is important to consider not only whether the proposed solutions would be effective to block illegal robocalls, but also whether they would be easy to use, and whether they could be rolled out in a timely manner. For example, a network-based solution could require extensive investment and active

---

if we want to refinance our VA loan. We have been on the Do Not Call list since 2006 and have asked them to stop calling us 6–8 times a day. They pointedly refuse to stop. This is not about freedom of speech, it is invasion of privacy. I, on behalf of many, many people request my Federal Government figure a way to make these people stop calling over and over again."

—Constituent from Yorktown, VA 08/27/2012

"My name is [redacted] and I reside in Charlottesville, VA. I am in the fourth grade. I am writing to ask that you help by intervening in the issue of unsolicited phone calls. Our number is on the Do Not Call list. In the last two days we've received three such calls."

—Constituent from Charlottesville, VA 05/23/2012

participation by carriers, which might make such a solution more difficult to roll out than a solution that consumers could implement on their own, with little or no reliance on carriers. In any event, the FTC actively encourages carriers to pursue all efforts to curb illegal robocalls, regardless of the specific technical approach or approaches adopted.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. DAN COATS TO LOIS GREISMAN

Question 1. I commend the work the Federal Communications Commission (FCC) and the Federal Trade Commission (FTC) have done in establishing a national Do-Not-Call Registry pursuant to their authorities under the Telephone Consumer Protection Act (TCPA). The registry is nationwide in scope, applies to all telemarketers (with the exception of certain non-profit organizations), and covers both interstate and intrastate telemarketing calls. Recently, I have heard a number of concerns from my state regarding the regulation of high volume auto-dialer initiated voice over Internet protocol (VOIP) "broadcasted" calls. My understanding is that these calls can put 10,000 calls per minute onto Indiana's landline telephone network, by using VOIP technology, in an attempt to get around Indiana's Do Not Call List. Does the technology exist to identify these high volume, auto-dialer initiated calls in real time?

Answer. I am not currently aware of any such identification technology that is broadly available to U.S. consumers. There are certain call-blocking "apps" that work only on wireless smartphones. The FTC launched the Robocall Challenge to encourage parties to create solutions that would identify and block illegal, high-volume, autodialed calls, which are generally made using voice over Internet protocol technology. The Challenge was designed to stimulate the marketplace to put such technological solutions into the hands of U.S. consumers, and we believe it was enormously fruitful. The winning solutions, including that of Aaron Foss, who testified at the hearing on July 10th, contained promising ideas about how to address illegal robocalls using a combination of call pattern analytics and crowd-sourced data.

Question 1a. My understanding is that when phone calls are made, there are usually two user-facing identifiable pieces of information: a phone number and a Caller ID Name (CNAM). I understand that the CNAM can be used to display the calling party's name alongside the phone number, to help users easily identify a caller. I have also been told that there are numerous CNAM lookup services which allow you to pay a small fee to lookup the CNAM of a specified caller (by phone number). Do any mechanisms exist to prevent telemarketers from blocking CNAM lookups by individuals?

Answer. I am unaware of any technological mechanisms that would prevent telemarketers from blocking CNAM lookups by individuals. However, with certain limited exceptions, a telemarketer violates the FTC's Telemarketing Sales Rule (TSR) if it fails to transmit an accurate telephone number and, when made available by the telemarketer's carrier, its CNAM, to any caller identification service used by the call recipient. 16 C.F.R. 310.4(a)(8). Thus, telemarketers violate the TSR if they block their telephone numbers, causing a consumer's caller ID or telephone to show "blocked" or "unavailable." In addition, it is illegal to assist and facilitate a practice prohibited by the TSR; such liability attaches if the entity knows or consciously avoids knowing of the prohibited activity. 16 C.F.R. 310.3(b). As a result, carriers or CNAM lookup services that help telemarketers hide their identities by providing false caller ID information or blocking the telemarketers' phone numbers, or that otherwise facilitate illegal activity, may be liable under the TSR.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. CLAIRE MCCASKILL TO ERIC J. BASH

Question 1. The FTC focuses on deceptive telemarketing through the lens of consumer protection. The FCC, as regulator of the telecommunications industry, brings its expertise on the wireline and wireless telephone networks themselves. Does the FCC have any concerns about or see any barriers to the winning technological solutions chosen by the FTC?

Answer. Henning Schulzrinne, the FCC's Chief Technology Officer, was one of three judges who determined the winners of the FTC-sponsored competition. Other FCC staff members have also spoken informally with the winners of the FTC Robocall Challenge to gain a better understanding of their winning ideas. We under-

stand that the winning ideas are currently in the development or implementation phases. While there are questions about some details, including whether caller ID spoofing may affect their use of caller ID information to identify robocallers, we believe the ideas are promising. The competition explicitly focused on ideas that could be implemented quickly, even if they could not suppress all illegal robocalls. Longer term approaches that increase the trustworthiness of caller ID information may make solutions such as those identified in the FTC-sponsored competition work even better.

Question 2. At the hearing, you said that additional legislation could be useful to better enforce against individuals or entities that provide or facilitate phony numbers used to spoof caller IDs. You also mentioned that the FCC has previously suggested revising the Truth in Caller ID Act to give the FCC direct regulatory authority over so-called third-party spoofing providers. From your agency's perspective, would changing the Truth in Caller ID Act be the most effective way for the FCC to help stop caller ID spoofing? Are there any other legislative solutions the FCC believes would better equip it to take enforcement actions against such entities or individuals?

Answer. In addition to recommending that Congress give the FCC authority to regulate third-party spoofing providers, the FCC has also suggested that Congress expand the Truth in Caller ID Act in several other ways, by:

- broadening the scope of the statute to prohibit spoofing by persons outside of the United States when directed at people inside the United States;
- clarifying whether the existing restrictions should apply to Voice over Internet Protocol providers that enable only outbound calls; and
- stating explicitly that text messaging is covered by the statute.

The FCC recommended that Congress take these additional steps to secure the integrity of telephone numbers as a reliable identifier of a call's origin, particularly as VoIP technology increasingly replaces the traditional technologies upon which telecommunication service is widely based, and as text messaging increasingly supplements voice communications.

Technological solutions that empower consumers to block illegal robocalls so that they do not receive them in the first instance may also be helpful in thwarting illegal robocalls. An industry standards organization is currently working with FCC technology staff to design a system whereby originating carriers and certain VoIP callers would cryptographically sign calls so that receiving carriers can validate that callers in fact have the right to use the telephone number they are using. The Commission staff hopes that the joint effort may lead to implementable specifications in about a year.

Question 3. The FCC's distinction in its rules for wireline and wireless phones stems from the Telephone Consumer Protection Act of 1991. Needless to say, the wireless industry has changed dramatically since then. Would revisiting that statute to eliminate the anachronistic distinction be something that would allow the FCC to be more aggressive in taking on fraudulent robocalls?

Answer. The restrictions on robocalls in the Telephone Consumer Protection Act (TCPA) and the FCC's implementing rules are generally stricter for calls to wireless numbers than to wireline/residential ones. Section 227(b)(1)(A) of the TCPA and FCC rules prohibit non-emergency autodialed or prerecorded calls to wireless numbers, regardless of content, without prior express consent. Section 227(b)(1)(B) and FCC rules prohibit prerecorded telemarketing calls to residential/wireline numbers without prior express consent. Neither autodialed calls nor purely informational calls are covered by the latter provision concerning calls to residential lines. (Note that the TCPA does not distinguish between fraudulent robocalls and other robocalls, for either residential/landline or wireless numbers; as such, while the Commission is certainly very concerned about fraudulent robocalls, whether a call is fraudulent is not an element of legal analysis under the TCPA.)

In light of increasing consumer reliance on wireless services since the TCPA was enacted more than twenty years ago, the distinctions in the statute between wireless and residential/wireline numbers may well be outdated. These distinctions can be a source of confusion to consumers, complicate compliance efforts for law-abiding callers and marketers, and introduce additional steps for law enforcement, in terms of both the factual discovery and legal analysis needed to investigate and pursue those who violate the law. As a result, harmonizing the legal standards that apply to robocalls to residential/wireline and wireless numbers may well benefit consumers, callers and telemarketers, as well as law enforcement.

Question 4. What are the limitations your agency faces in bringing more enforcement cases? Is there a need for legislation to assist your efforts?

Answer. As discussed at the hearing, two major impediments to the FCC taking stronger enforcement action against illegal robocallers are the difficulty of identifying wrongdoers, and limitations on the FCC's power. Amendments to the Truth in Caller ID Act such as those the FCC has proposed (see above), coupled with development and implementation of technological means to improve caller ID authentication (also discussed above), would help to address the first of the FCC's enforcement challenges. Congress could enhance the FCC's enforcement powers against illegal robocallers by making it easier for the agency to impose significant forfeitures, in at least three ways: (1) allow the FCC to impose a forfeiture on a non-licensee robocaller without first issuing a citation; (2) extend the current statute of limitations from one year to at least two; (3) increase the maximum forfeiture that the agency can impose on non-licensee robocallers.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. AMY KLOBUCHAR TO ERIC J. BASH

Question. Ms. Greisman and Mr. Bash, we know that technology will continue to evolve. How are the FTC and the FCC working to keep up with these evolutions in communications to protect consumers from future scamming operations?

Answer. The Commission recognized in 2003 and 2008 orders that "[i]t is clear from the statutory language and the legislative history that Congress anticipated that the FCC, under its TCPA rulemaking authority, might need to consider changes in technologies." In those orders, the Commission made it clear that as automated calling moved away from random or sequential dialing, the TCPA could still be applied to newer or different calling technologies, including predictive dialers that relied more primarily on defined lists of telephone numbers rather than random or sequential dialing. We will continue to monitor and address new technologies in this area as warranted, and Commission staff is actively fostering industry standards that, in the long term, should help to reduce the number of illegal robocalls and the malicious caller ID spoofing often associated with them. In the short term, we also plan to work with key telecommunication providers to address the problem of consumers being inundated with calls if their numbers happen to be used as caller ID by illegal robocallers.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MARK WARNER TO ERIC J. BASH

Question 1. Over the past year or so, my office has seen a marked increase in calls and letters regarding possible abuses by some telemarketers. Since January 2013, my office has heard from more than 300 people requesting assistance with the Do Not Call List, and since taking office in 2009, my office has heard from over 1200 people on this issue. A small sampling of some of the concerns we have received are also included in this document for the record.*

---

* Selected Constituent Robocall Concerns

"It is an invasion of our privacy, and it ties up our phones and disrupts our lives to get as many as 15 calls every single day when we have been on the donotcall list since day 1. Anything you can do about this issue will be greatly appreciated."

—Constituent from Arlington, VA 5/26/2012

"I am registered on the "Do Not Call" list for my home phone (not cellphone) and I am still getting many solicitation "robo calls" for lower credit card rates, car warranties, and other commercial products. Some callers block caller ID. I systematically report these callers via the "report a violator" process on the Registry website. I have been on the do-not-call registry since its inception, and I have verified this on the Registry site. I also put my elderly mother's home phone number on the DNC Registry several years ago. She also gets many solicitation calls. I am well versed on the types of calls that the DNC system is supposed to address, and the kinds of calls that are excepted. I am astonished at the number of calls I am getting even as I am on the DNC list."

—Constituent from Fairfax, VA 05/04/2012

"xxx-xxx-xxxx [redacted]. This number continues to call with impunity, even though they are on my FTC Do Not Call Registry, and several other residents I'm friends with. They are scam artists, trying to mine personal information, and the FTC hasn't responded to my concerns. Are you game for going after this group of obvious scammers, because a lot of vulnerable citizens, could be prey for their scam which involves lowering debt. They call themselves [redacted], and they are a company I and others have never done business with. Thank you kindly."

—Constituent from Fairfax, VA 06/06/2012

As a supporter of the Do Not Call Act, I sympathize with the frustration of my constituents. I recognize that the same technology that is allowing telephone service providers to more efficiently manage networks is also enabling disreputable callers to abuse the system.

Still, it seems to me that if we can't find a technical solution to abusive telemarketing calls, that raises many serious questions as well. I encourage you to think more creatively about possible solutions, and about any legislative authorities that would better enable the FTC to keep pace with technology. For instance, have similar problems occurred in other countries? If so, are there any solutions adopted in other markets that might be applicable in the U.S.?

Answer. The Commission staff has previously discussed telemarketing and related consumer issues with its Canadian counterparts, to the mutual benefit of both groups. Our recent research shows that, in addition to Canada, the United Kingdom, Australia, and India have all addressed problems with unwanted telemarketing calls to consumers. For example, the UK has a "Telephone Preference Service," which appears to be similar to our National Do-Not-Call Registry. Similarly, India and Australia also have do-not-call lists. In the UK, a technology is available that blocks all calls until the caller enters an identifying phone number, thereby establishing that the call is a human-originated call rather than a robocall. In Canada, a blocking service has been implemented that is aimed at stopping unwanted calls from known robocall or telemarketer numbers, based, in part, on filtering technology that relies on telemarketers identified by consumers (*i.e.,* crowd-sourced). While we must, of course, focus on the specific statutory requirements of the TCPA, we will also continue to monitor the situations in other countries to ensure that we are aware of solutions that they may develop to problems that we have in common.

Question 2. In 2012, the Federal Trade Commission (FTC) challenged innovators to come up with a solution that would block illegal commercial robocalls on landlines and mobile phones. One of the proposed solutions creates a filtering system, similar to an e-mail spam filter, that intercepts and filters out illegal robocalls using a technology that "blacklists" and "whitelists" phone numbers. The proposal envisions a consumer-facing system, however, others have suggested that a network-based system might be more efficient and less burdensome for consumers. Do you believe that a filtering system would be effective? If so, do you believe it should be implemented by networks or by consumers? If not, do you have ideas for a better solution?

Answer. The FCC staff spoke informally with the winners of the FTC Robocall Challenge, and we understand that the winning ideas are currently in the development or implementation phases. There are questions about some details, including whether caller ID spoofing may affect their use of caller ID information to identify robocallers, and they may work better if the integrity of caller ID can be improved.

"I have been getting calls on my home phone from a 'Credit Card Services' for over a year now. I have submitted at least five complaints on the FTC website and at least two complaints' on the 'Do Not Call' website. I have asked to speak to a supervisor numerous times, only to be hung up on. I have told them over and over and over again to not call me. I have threatened them with FTC complaints. I have received over 30 calls from this company and have turned in many complaints to the Federal Trade Commission and nothing seems to work. If you look on the internet, you will see tens of thousands of complaints. Therefore, I would like to request that you (my congressmen) get the Federal Trade Commission to do their job and shut these people down."

—Constituent from Alexandria, VA 07/23/2012

"Over the last couple of months, I've been getting an increasing number of robo-dialer/recorded commercial calls in violation of the Do-Not-Call registry. Many have been from the same 'crook', often "Credit Card Services." I've reported most of them on the FTC's Do Not Call registry. (That is not counting the growing number of political calls, which unfortunately are not violations of Do Not Call)."

—Constituent from Reston, VA 08/20/2012

"Senator—Please have someone on your staff Google (xxx)xxx-xxxx [redacted] and you will see several websites dedicated to complaints about harassing phone calls from this number asking if we want to refinance our VA loan. We have been on the Do Not Call list since 2006 and have asked them to stop calling us 6–8 times a day. They pointedly refuse to stop. This is not about freedom of speech, it is invasion of privacy. I, on behalf of many, many people request my Federal Government figure a way to make these people stop calling over and over again."

—Constituent from Yorktown, VA 08/27/2012

"My name is [redacted] and I reside in Charlottesville, VA. I am in the fourth grade. I am writing to ask that you help by intervening in the issue of unsolicited phone calls. Our number is on the Do Not Call list. In the last two days we've received three such calls."

—Constituent from Charlottesville, VA 05/23/2012

We will continue to monitor the progress of these proposed solutions, including whether they should be implemented on telecommunications networks or by consumers, or through a combination of the two approaches. We will also work with telecommunication service providers to encourage the development of open interfaces that allow third-party services to offer innovative ways for consumers to manage their incoming phone calls.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. DAN COATS TO ERIC J. BASH

Question 1. I commend the work the Federal Communications Commission (FCC) and the Federal Trade Commission (FTC) have done in establishing a national Do-Not-Call Registry pursuant to their authorities under the Telephone Consumer Protection Act (TCPA). The registry is nationwide in scope, applies to all telemarketers (with the exception of certain non-profit organizations), and covers both interstate and intrastate telemarketing calls. Recently, I have heard a number of concerns from my state regarding the regulation of high volume auto-dialer initiated voice over Internet protocol (VOIP) "broadcasted" calls. My understanding is that these calls can put 10,000 calls per minute onto Indiana's landline telephone network, by using VOIP technology, in an attempt to get around Indiana's Do Not Call List. Does the technology exist to identify these high volume, auto-dialer initiated calls in real time?

Answer. Technology exists that can identify—and block—a high-volume of calls in certain instances, such as calls originating from a single number, or sharing the same electronic signature, such as call length, call source and destination numbers, or certain VoIP call attributes. Large businesses often purchase this type of technology to protect their corporate networks from voice SPAM, VoIP Denial of Service attacks, and other activities the business seeks to prevent.

Question 1a. My understanding is that when phone calls are made, there are usually two user-facing identifiable pieces of information: a phone number and a Caller ID Name (CNAM). I understand that the CNAM can be used to display the calling party's name alongside the phone number, to help users easily identify a caller. I have also been told that there are numerous CNAM lookup services which allow you to pay a small fee to lookup the CNAM of a specified caller (by phone number). Do any prohibitions exist to prevent this practice by telemarketers?

Answer. CNAM databases link Calling Party Numbers (CPNs) to the individuals and entities to whom the numbers have been assigned. Some terminating providers maintain their own CNAM database and others purchase CNAM database services from third-party providers that aggregate the listing information from a variety of sources. Typically this aggregation is done with real-time information feeds and may involve a chain of feeds through several layers of providers and resellers. When a phone call is made, Caller ID services often dip into the CNAM database to look up the name or other identifying information of the caller. We are not aware of any specific legal restrictions prohibiting access to CNAM databases. Commission staff would be happy to discuss these issues in further detail with your staff.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. CLAIRE MCCASKILL TO KEVIN G. RUPY

Question 1. Your member companies are by no means the problem, but I believe your industry should be more proactive in being part of the solution if we are going to seriously address the proliferation of fraudulent robocalls. In your testimony, you described past and present actions of providers to help combat the problem. Do you believe your industry has done as much as it could or should to assist law enforcement and consumers? Why or why not?

Answer. Yes, we believe our industry does as much as it can to assist both law enforcement and consumers in this regard. The telecommunications industry is, along with the consumer, a victim of unwanted calls that annoy consumers and diminish the value and stability of telecommunications services. Unfortunately, a large number of criminals, now able to use cybercrime techniques and international boundaries to evade national jurisdiction, present challenges to law enforcement, consumers and industry alike. The telecommunications industry is highly motivated to control abuse, and is responding to the growth of abuse by creating the right technologies, systems and processes to mitigate it. Industry is not only assisting, but in most cases leading enforcement, technology development and collaborative actions needed to address this issue.

USTelecom members have long worked collectively and coordinated with private and government stakeholders to address issues relating to illegal robocalls. For example, in a 2010 FTC action against a robocaller that in one year made more than 370 million calls to consumers nationwide, the agency specifically acknowledged the help that USTelecom member companies AT&T and Verizon provided in the investigation and resolution of the case.

In terms of assistance to our customers, no area is more challenging to address than mass calling events originating outside of our networks over multiple IP-based platforms using spoofed caller ID, many of which involved auto-dialers or pre-recorded human voices, often referred to as robocalls. Since no technology currently exists that enables carriers to identify in real time whether any single call traversing their network is legitimate or illegitimate, it is not currently practical to deploy services that can identify the illegal robocall needle in the high-volume call traffic haystack. As reflected in Attachment One, carriers have no way of distinguishing between legal or illegal robocalls that may be terminating on their network—only the consumer is in a position to make that determination.

Nevertheless, carriers do their best to protect their customers in the context of suspicious mass calling events, as outlined in greater detail in our answer to your next question. Our members have long been providing—and will continue to develop—various services consumers can use to help mitigate the robocall problem. The scope and availability of these services differ by carrier, but may include basic caller-ID functionality, conditional call-forwarding, anonymous call-blocking, block lists and other related services. Unfortunately, these services are susceptible to evasion by caller-ID spoofing, which can be accomplished at relatively low cost from anywhere in the world using readily available technologies such as a personal computer and free software.

Question 2. Mr. Rupy, you explained at the hearing that your member companies' network operations centers monitor call traffic over their networks and initiate investigations into suspicious mass-calling events. You also added that your member companies address such suspicious mass-calling events through different measures. Could you provide specific details on what measures your member companies take when they notice a suspicious mass-calling event?

Answer. As discussed in our testimony, many USTelecom member companies maintain network operations centers that monitor network traffic, conduct traffic data forensics and initiate mass-calling investigations. During suspected mass-calling events, providers can undertake various measures to mitigate their effect, including routing traffic to an alternate tandem, and coordinating with the providers sending the incoming traffic. For example, when a carrier realizes that a connecting provider is sending an unusually large amount of traffic onto its network, it may contact the connecting provider to request that its customer cease generating the traffic. Of course, given the interconnected nature of the Internet and the public switched telephone network, the company delivering the large call-traffic volume may be only one of several intermediaries simply passing along traffic received from yet another provider.

Finally, many companies maintain call fraud bureaus that will initiate investigations after a suspected mass calling event. Using traffic data forensics and other investigative tools, providers will try to identify the parties behind a particular mass calling event. When they can identify the entities behind these calls, USTelecom's members have sued the perpetrators, and often engage law enforcement agencies and the Federal Trade Commission to investigate and prosecute illegal robocall incidents.

Question 3. What issues, specifically, with regards to robocalls are the standards-setting groups you cited in your testimony addressing that would better protect American consumers from fraudulent robocalls? What kinds of solutions and best practices have been and will be adopted by industry members to address the robocall problem?

Answer. USTelecom's member companies have an extensive record of working with standards-setting groups and other industry associations to address robocalls. In particular, they have worked with and continue to work with the Alliance for Telecommunications Industry Solutions (ATIS) to develop standards and best practices to address the robocall problem, with the Internet Engineering Task Force (IETF) to develop standards for secure call authentication and with the Communications Fraud Control Association (CFCA) to combat communications fraud.

ATIS has developed various guidelines and best practices that help network management personnel address traffic management issues that may arise during mass calling events. For example, ATIS helped public safety agencies optimize their deployment of Emergency Notification Systems to better ensure call completion with-

out overwhelming affected networks. ATIS has also published reference information for responsible companies on the use of auto-dialers, and will publish an updated section related to network security later this year. ATIS is also planning to update existing documents as they relate to the deployment of next generation networks in order to address various network management issues, including mass calling events.

The IETF is the standards organization responsible for most Voice over Internet Protocol (VoIP) standards. The IETF has formed an active Secure Telephone Identity Revisited (STIR) Working Group, whose priority will be to develop standards for use in IP-based communications networks for authenticating callers.

Through public-private partnerships like the CFCA, industry stakeholders work alongside law enforcement to identify best practices and solutions to a broad range of telecommunications-related issues, including robocalls. Given its collaborative public-private nature, the CFCA fosters critical relationships between individual industry stakeholders and law enforcement. These professional relationships are crucial to investigating and prosecuting individuals that engage in fraudulent activities occurring over communications networks, including illegal robocalls.

The CFCA also provides a forum for industry stakeholders and law enforcement to coordinate on issues relating to the latest scams, evolving investigations and cases, and other related fraud matters. This invaluable coordination increases the abilities of public and private stakeholders to stay ahead of the constantly evolving robocall environment, and thereby more effectively combat the bad actors operating in this area.

Question 4. In their written and oral testimony, witnesses from the FTC and the FCC proposed a number of statutory changes that would better equip their agencies to combat fraudulent robocalls. For inclusion in the hearing record, I ask that you provide your comments on the following proposed statutory changes by September 9, 2013: Elimination of the Federal Trade Commission Act's common carrier exemption.

Answer. As Chairwoman McCaskill noted in her August 16, 2013 letter to USTelecom, in the area of fraudulent robocalls "America's telecommunications providers are not the problem." We agree, and believe that this makes the elimination of the common carrier exception somewhat beside the point. Because the FCC already has full authority to pursue appropriate remedies against carriers, USTelecom is concerned that elimination of the common carrier exception could lead to regulation of the communications industry by two separate agencies, thereby creating the potential for duplicative or conflicting regulatory requirements, resulting in additional consumer confusion and frustration. More broadly, robocalls are among the many issues that USTelecom maintains requires Congress to create a new framework that reflects today's converged technological world.

Question 4a. Changes to the FCC's enforcement authorities including:

- Allowing the FCC to impose a forfeiture on non-licensee robocalls violators without first issuing citation;

Answer. USTelecom supports full enforcement of relevant laws by agencies against entities engaging in illegal robocall activities. The FTC already has authority to enforce existing Do-Not-Call provisions, including the authority to seek civil penalties, restitution for victims of telemarketing scams and disgorgement of ill-gotten gains. As discussed below, USTelecom believes that in lieu of incremental approaches, Congress should instead focus on a new framework that better reflects the realities of today's converged marketplace.

(b) Expanding the statute of limitations from one year to at least two years; and

Answer. Given the immediacy of illegal robocalling incidents, the current one year time-frame on the statute of limitations is sufficient for ensuring that ample time is available to investigate and prosecute such incidents.

(c) Increasing the maximum forfeiture that the FCC can impose on non-licensee robocallers.

Answer. It is unlikely that increasing the maximum forfeiture available to the FCC will favorably impact the proliferation of these calls. In instances where such calls are originating from overseas, the threat of increased forfeitures will likely have no effect on the decision to engage in such activities. The better alternative is for the FCC to more aggressively pursue and prosecute bad actors operating in this area.

Question 4b. Revisions to the Truth-In-Caller ID Act [of 2009] including:

Answer. In light of the evolving, interconnected and interdependent global Internet network of networks, USTelecom cannot vouch for the efficacy of any of these proposals. However, USTelecom supports targeted and enhanced enforcement efforts that specifically target the entities engaged in illegal robocall activity. USTelecom

pledges to continue to work with policymakers to address the problem and to cooperate in government enforcement actions against firms and individuals that abuse our open communications networks in order to perpetrate fraud on consumers, enterprise, and carriers alike.

- Expanding the scope of the prohibition to apply to persons outside of the United States when spoofing is directed at people inside the United States;

Answer. USTelecom does not support expanding the Truth in Caller-ID Act of 2009 prohibitions to persons outside of the United States when spoofing is directed at people inside the United States. Significant jurisdictional issues would arise from the application of domestic law to international operators, and it is therefore highly questionable whether efforts to enforce such prohibitions would be effective. In addition, it is possible that such an expansion of domestic law could encourage other countries to pass extra-territorial laws to the detriment of both consumers and U.S.-based companies providing communications or other consumer services abroad.

(b) Clarifying whether the existing restrictions should apply to VoIP providers that enable only outbound calls; and

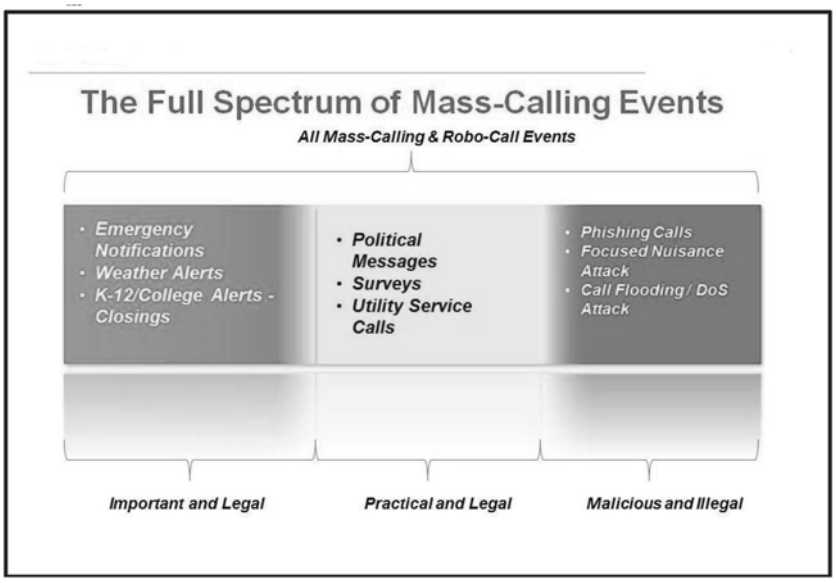
Answer. USTelecom does not oppose the FCC clarifying that the regulations relating to the Truth in Caller-ID Act of 2009 apply to VoIP providers that enable only outbound calls, to the extent such an ambiguity currently exists.

(c) Giving the FCC authority to regulate third-party spoofing services.

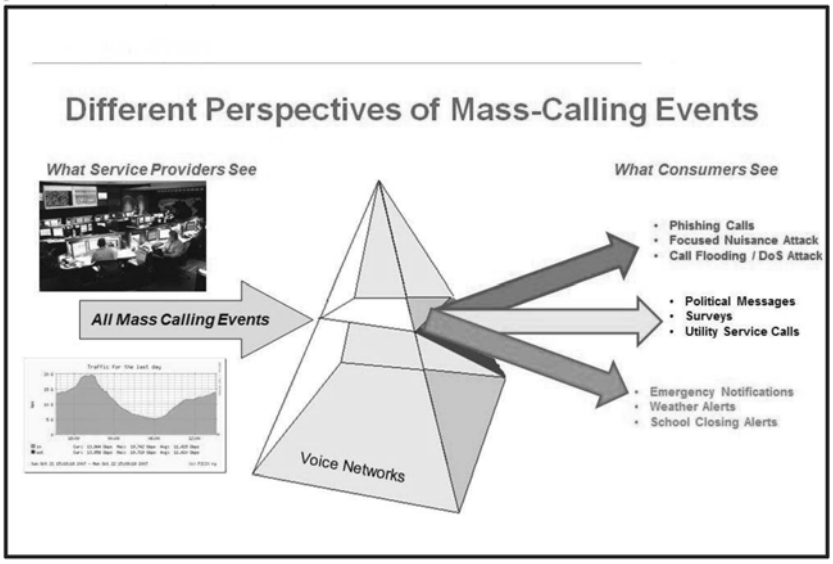
Answer. The FCC already has the authority to regulate third-party spoofing services. In its 2010 order addressing caller-ID spoofing, the FCC declined to impose additional obligations on such third-party caller ID services. It stated, however, that its decision to do so "in no way immunizes them from the obligation to comply with the Act." The FCC further stated that where a third-party caller ID spoofing service causes the transmission or display of false or misleading caller ID information with the intent to defraud, cause harm, or wrongfully obtain anything of value, "such service will be in violation of the Truth in Caller ID Act and our rules."

The solutions proposed in each of these questions are at best incremental approaches that reflect increasingly obsolete statutes in the context of today's rapidly evolving technological world. Robocalls are among the many issues that USTelecom maintains require Congress to create a new framework reflecting today's converged technologies. It is doubtful that the drafters of the Federal Trade Commission Act, the Communications Act, the Telephone Consumer Protection Act, or other similar statutes ever envisioned circumstances under which functionally equivalent services would be regulated by separate Federal agencies, sometimes applying different standards and consumer protections, even though those services could be delivered through technologies that often cannot be constrained by state or national boundaries. USTelecom hopes the Committee will begin the process of developing legislation that would remedy these types of circumstances with the goal of developing a pro-consumer, pro-competitive framework for the Information Age.

ATTACHMENT ONE



ATTACHMENT ONE (CON'T)



RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MARK WARNER TO KEVIN G. RUPY

Question 1. Over the past year or so, my office has seen a marked increase in calls and letters regarding possible abuses by some telemarketers. Since January 2013, my office has heard from more than 300 people requesting assistance with the Do Not Call List, and since taking office in 2009, my office has heard from over 1200 people on this issue. A small sampling of some of the concerns we have received are also included in this document for the record.*

As a supporter of the Do Not Call Act, I sympathize with the frustration of my constituents. I recognize that the same technology that is allowing telephone service providers to more efficiently manage networks is also enabling disreputable callers to abuse the system.

Still, it seems to me that if we can't find a technical solution to abusive telemarketing calls, that raises many serious questions as well. I encourage you to think more creatively about possible solutions, and about any legislative authorities that would better enable the FTC to keep pace with technology. For instance, have similar problems occurred in other countries? If so, are there any solutions adopted in other markets that might be applicable in the U.S.?

---

* Selected Constituent Robocall Concerns

"It is an invasion of our privacy, and it ties up our phones and disrupts our lives to get as many as 15 calls every single day when we have been on the donotcall list since day 1. Anything you can do about this issue will be greatly appreciated."

—Constituent from Arlington, VA 5/26/2012

"I am registered on the "Do Not Call" list for my home phone (not cellphone) and I am still getting many solicitation "robo calls" for lower credit card rates, car warranties, and other commercial products. Some callers block caller ID. I systematically report these callers via the "report a violator" process on the Registry website. I have been on the do-not-call registry since its inception, and I have verified this on the Registry site. I also put my elderly mother's home phone number on the DNC Registry several years ago. She also gets many solicitation calls. I am well versed on the types of calls that the DNC system is supposed to address, and the kinds of calls that are excepted. I am astonished at the number of calls I am getting even as I am on the DNC list."

—Constituent from Fairfax, VA 05/04/2012

"xxx-xxx-xxxx [redacted]. This number continues to call with impunity, even though they are on my FTC Do Not Call Registry, and several other residents I'm friends with. They are scam artists, trying to mine personal information, and the FTC hasn't responded to my concerns. Are you game for going after this group of obvious scammers, because a lot of vulnerable citizens, could be prey for their scam which involves lowering debt. They call themselves [redacted], and they are a company I and others have never done business with. Thank you kindly."

—Constituent from Fairfax, VA 06/06/2012

"I have been getting calls on my home phone from a 'Credit Card Services' for over a year now. I have submitted at least five complaints on the FTC website and at least two complaints' on the 'Do Not Call' website. I have asked to speak to a supervisor numerous times, only to be hung up on. I have told them over and over and over again to not call me. I have threatened them with FTC complaints. I have received over 30 calls from this company and have turned in many complaints to the Federal Trade Commission and nothing seems to work. If you look on the internet, you will see tens of thousands of complaints. Therefore, I would like to request that you (my congressmen) get the Federal Trade Commission to do their job and shut these people down."

—Constituent from Alexandria, VA 07/23/2012

"Over the last couple of months, I've been getting an increasing number of robo-dialer/recorded commercial calls in violation of the Do-Not-Call registry. Many have been from the same 'crook', often "Credit Card Services." I've reported most of them on the FTC's Do Not Call registry. (That is not counting the growing number of political calls, which unfortunately are not violations of Do Not Call)."

—Constituent from Reston, VA 08/20/2012

"Senator—Please have someone on your staff Google (xxx)xxx-xxxx [redacted] and you will see several websites dedicated to complaints about harassing phone calls from this number asking if we want to refinance our VA loan. We have been on the Do Not Call list since 2006 and have asked them to stop calling us 6–8 times a day. They pointedly refuse to stop. This is not about freedom of speech, it is invasion of privacy. I, on behalf of many, many people request my Federal Government figure a way to make these people stop calling over and over again."

—Constituent from Yorktown, VA 08/27/2012

"My name is [redacted] and I reside in Charlottesville, VA. I am in the fourth grade. I am writing to ask that you help by intervening in the issue of unsolicited phone calls. Our number is on the Do Not Call list. In the last two days we've received three such calls."

—Constituent from Charlottesville, VA 05/23/2012

Answer. Given the interdependent, interconnected, and global nature of the Internet, we would suspect that unwanted robocalls are an international issue. While USTelecom is not familiar with the availability, effectiveness, or nature of solutions adopted in other countries, the association and its member companies were interested in the testimony that a Canadian company provided to the Subcommittee regarding the deployment of a patented technology to address unwanted robocalls. Our member companies are seeking more information about this technology. However, as noted in our testimony and below, American law governing common carrier and privacy obligations with regard to voice telephone calls, together with consumers' historical needs and expectations with regard to call completion, may not make every international comparison useful, even if a particular solution can be implemented under another nation's laws or traditions.

Question 2. In 2012, the Federal Trade Commission (FTC) challenged innovators to come up with a solution that would block illegal commercial robocalls on landlines and mobile phones. One of the proposed solutions creates a filtering system, similar to an e-mail spam filter, that intercepts and filters out illegal robocalls using a technology that "blacklists" and "whitelists" phone numbers. The proposal envisions a consumer-facing system, however, others have suggested that a network-based system might be more efficient and less burdensome for consumers. Do you believe that a filtering system would be effective? If so, do you believe it should be implemented by networks or by consumers? If not, do you have ideas for a better solution?

Answer. Our member companies are providing—and will continue to develop—various technologies and services to help mitigate the robocall problem. These include basic caller-ID functionality, enhanced caller authentication and authorization, conditional call-forwarding, anonymous call-blocking, and other services that may vary by provider.

The rapid and ever-changing nature of the robocall problem, however, makes the potential for a technological "silver bullet," such as a filtering system, highly problematic. An open communications network is inherently vulnerable to abuse. This abuse can be managed, but (as explained below) only at the expense of some legitimate calls being delayed or blocked. The existing legal framework for phone calls under which USTelecom members operate generally does not permit such delaying or blocking. For example, USTelecom member companies in recent months have been working with Federal and state authorities on ways to mitigate the effects of criminal Telephony Denial of Service (TDoS) attacks directed towards public safety answering points (PSAPs). During such events, telephone providers may implement corrective measures to alleviate overwhelming call volumes. However, such corrective measures cannot be applied more broadly. For example, in the event a carrier inadvertently blocks a legitimate and critical robocall (*e.g.,* one *originating* from a public safety entity), the positive public service aspects of such legitimate calls would be negated.

Therefore, policymakers should proceed cautiously when contemplating the creation or facilitation of regimes using yet-to-be developed technologies that could prevent critical—possibly life-saving—information from reaching the public. This is particularly challenging due to the relative ease with which illegal robocallers can "spoof" legitimate phone numbers. Spoofing technology can easily fool consumers into taking calls they should avoid. For example, spoofing the number of the local municipal hospital can dupe a senior citizen into believing that a fraudulent effort to sell phony medical products or services is actually a legitimate call from a whitelisted number. In addition, solutions implementing call blocking features based upon a whitelist could potentially block an important—albeit unexpected—message from a legitimate caller. Conversely, solutions that rely extensively on blocking calls populated by a blacklist could very well result in the blocking of legitimate calls from callers whose own phone numbers have been illegally spoofed.

The blocking of select phone calls based on CNAM data is fraught with risk since it is impossible to identify legitimate robocalls from illegitimate robocalls as they are occurring. In particular, public safety agencies are increasingly using automated phone calls for "push-911" services. Such systems send a recorded message to phone numbers en masse, listed and unlisted, in a geographical calling area. They have been used by public safety entities to great effect, most recently when residents of Watertown, Massachusetts, were advised by public safety agencies to shelter in place when their neighborhood became the epicenter of the manhunt for one of the Boston Marathon bombing suspects.

Even non-public safety entities utilize robocalls for public safety purposes. For example, KFOR–TV, the NBC affiliate for Oklahoma City, Oklahoma, instituted the "4Warn" storm alert system, a free public service that allows Oklahoma residents to opt in to receive a voice message on their home, office or cell phone any time

there is a tornado warning issued in their county. More than 34,000 people have signed up for the 4Warn service. During a 2010 tornado event, the service was used to send more than 28,000 warnings in less than 24 hours.

A better solution to filtering, which appeared to be the consensus of the regulatory participants in last fall's FTC robocall workshop, would be the development of strong caller authentication and authorization mechanisms within the industry that will enable better management of the problem. The development of standards in this area for use in IP-based communications networks is the priority of the STIR Working Group recently activated within the IETF. However, such solutions are dependent upon a full transition to IP-based communications networks, a process that is currently in the early stages.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. DAN COATS TO KEVIN G. RUPY

Question 1. Does the technology exist to identify high volume, auto-dialer initiated calls in real time?

Answer. While high-volume and random or sequential calling patterns can be identified, there are no currently available technologies that can reliably identify in real time whether calls are being initiated by auto-dialers, or what types of software and/or hardware are being used to initiate such calls. Moreover, given a mix of human-dialed calls from individual consumers, call centers and similar mass-calling locations (*e.g.,* political campaign headquarters) and auto-dialer initiated calls spoofing legitimate numbers, current technologies cannot reliably distinguish between the two, nor between legal and illegal mass calling events.

Question 2. Do any prohibitions exist to prevent a telemarketer from purchasing CNAM data?

Answer. USTelecom is not aware of any existing statutory or regulatory prohibitions preventing a telemarketer from purchasing CNAM data.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. CLAIRE MCCASKILL TO MICHAEL F. ALTSCHUL

Question. Your member companies are by no means the problem, but I believe your industry should be more proactive in being part of the solution if we are going to seriously address the proliferation of fraudulent robocalls. In your testimony, you described past and present actions of providers to help combat the problem. Do you believe your industry has done as much as it could or should to assist law enforcement and consumers? Why or why not?

Answer. The wireless industry is proud of its ongoing record of providing assistance to law enforcement. In particular, the FTC has noted the industry's assistance and cooperation ("The Commission would like to acknowledge the extraordinary cooperation that telecommunications carriers AT&T Mobility and Verizon Wireless provided in the investigation of the case." See *http://www.ftc.gov/opa/2009/05/robocalls.shtm.* Also, "The FTC acknowledges the invaluable assistance it received from Verizon Wireless, AT&T, and CTIA—The Wireless Association in this matter." See *http://www.ftc.gov/opa/2011/02/loan.shtm.*)

As I noted in my testimony, the wireless industry also has conducted its own investigations and brought lawsuits under the TCPA when they have been able to find the violators in the United States. Unfortunately, carriers experience the same difficulties law enforcement encounters in trying to trace calls to their source—these robocallers "spoof" caller ID, use proxy servers, and route calls through multiple networks, which, together, make it time consuming and often impossible to trace the source of these calls back to their origin.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MARK WARNER TO MICHAEL F. ALTSCHUL

Question 1. Over the past year or so, my office has seen a marked increase in calls and letters regarding possible abuses by some telemarketers. Since January 2013, my office has heard from more than 300 people requesting assistance with the Do Not Call List, and since taking office in 2009, my office has heard from over 1200

people on this issue. A small sampling of some of the concerns we have received are also included in this document for the record.*

As a supporter of the Do Not Call Act, I sympathize with the frustration of my constituents. I recognize that the same technology that is allowing telephone service providers to more efficiently manage networks is also enabling disreputable callers to abuse the system.

Still, it seems to me that if we can't find a technical solution to abusive telemarketing calls, that raises many serious questions as well. I encourage you to think more creatively about possible solutions, and about any legislative authorities that would better enable the FTC to keep pace with technology. For instance, have similar problems occurred in other countries? If so, are there any solutions adopted in other markets that might be applicable in the U.S.?

Answer. Both in light of Primus' testimony at July's hearing and the fact that many robocalling operations, when ultimately identified, are located off-shore, it is likely that this phenomena has an international dimension to it. However, because CTIA's focus is domestic in nature, we do not have great familiarity with what solutions or attempted solutions may have been used in other markets. Additionally, even if technology solutions are deployed successfully in other markets, they would need to be evaluated to determine whether they could be deployed here in a manner that would be consistent with wireless carriers' regulatory and legal obligations.

---

* Selected Constituent Robocall Concerns

"It is an invasion of our privacy, and it ties up our phones and disrupts our lives to get as many as 15 calls every single day when we have been on the donotcall list since day 1. Anything you can do about this issue will be greatly appreciated."

—Constituent from Arlington, VA 5/26/2012

"I am registered on the "Do Not Call" list for my home phone (not cellphone) and I am still getting many solicitation "robo calls" for lower credit card rates, car warranties, and other commercial products. Some callers block caller ID. I systematically report these callers via the "report a violator" process on the Registry website. I have been on the do-not-call registry since its inception, and I have verified this on the Registry site. I also put my elderly mother's home phone number on the DNC Registry several years ago. She also gets many solicitation calls. I am well versed on the types of calls that the DNC system is supposed to address, and the kinds of calls that are excepted. I am astonished at the number of calls I am getting even as I am on the DNC list."

—Constituent from Fairfax, VA 05/04/2012

"xxx-xxx-xxxx [redacted]. This number continues to call with impunity, even though they are on my FTC Do Not Call Registry, and several other residents I'm friends with. They are scam artists, trying to mine personal information, and the FTC hasn't responded to my concerns. Are you game for going after this group of obvious scammers, because a lot of vulnerable citizens, could be prey for their scam which involves lowering debt. They call themselves [redacted], and they are a company I and others have never done business with. Thank you kindly."

—Constituent from Fairfax, VA 06/06/2012

"I have been getting calls on my home phone from a 'Credit Card Services' for over a year now. I have submitted at least five complaints on the FTC website and at least two complaints' on the 'Do Not Call' website. I have asked to speak to a supervisor numerous times, only to be hung up on. I have told them over and over and over again to not call me. I have threatened them with FTC complaints. I have received over 30 calls from this company and have turned in many complaints to the Federal Trade Commission and nothing seems to work. If you look on the internet, you will see tens of thousands of complaints. Therefore, I would like to request that you (my congressmen) get the Federal Trade Commission to do their job and shut these people down."

—Constituent from Alexandria, VA 07/23/2012

"Over the last couple of months, I've been getting an increasing number of robo-dialer/recorded commercial calls in violation of the Do-Not-Call registry. Many have been from the same 'crook', often "Credit Card Services." I've reported most of them on the FTC's Do Not Call registry. (That is not counting the growing number of political calls, which unfortunately are not violations of Do Not Call)."

—Constituent from Reston, VA 08/20/2012

"Senator—Please have someone on your staff Google (xxx)xxx-xxxx [redacted] and you will see several websites dedicated to complaints about harassing phone calls from this number asking if we want to refinance our VA loan. We have been on the Do Not Call list since 2006 and have asked them to stop calling us 6–8 times a day. They pointedly refuse to stop. This is not about freedom of speech, it is invasion of privacy. I, on behalf of many, many people request my Federal Government figure a way to make these people stop calling over and over again."

—Constituent from Yorktown, VA 08/27/2012

"My name is [redacted] and I reside in Charlottesville, VA. I am in the fourth grade. I am writing to ask that you help by intervening in the issue of unsolicited phone calls. Our number is on the Do Not Call list. In the last two days we've received three such calls."

—Constituent from Charlottesville, VA 05/23/2012

Question 2. In 2012, the Federal Trade Commission (FTC) challenged innovators to come up with a solution that would block illegal commercial robocalls on landlines and mobile phones. One of the proposed solutions creates a filtering system, similar to an e-mail spam filter, that intercepts and filters out illegal robocalls using a technology that "blacklists" and "whitelists" phone numbers. The proposal envisions a consumer-facing system, however, others have suggested that a network-based system might be more efficient and less burdensome for consumers. Do you believe that a filtering system would be effective? If so, do you believe it should be implemented by networks or by consumers? If not, do you have ideas for a better solution?

Answer. Many of the filtering systems submitted for evaluation in the FTC's "Robocall Challenge" contest were based on Caller ID, which is easily spoofed, notwithstanding the fact that such spoofing is illegal. Given this vulnerability, I am skeptical that they will work. Additionally, to the extent that filtering systems were deployed at the network level, they would require carriers to screen the content of traffic addressed to their customers, something very likely to raise privacy concerns. And finally, even if carriers screened traffic, it could still be difficult to identify and separate "bad" robomessages from "good" auto-dialed messages such as a high volume of identical messages announcing airline flight delays or a school system letting families know of a weather delay or cancellation.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. DAN COATS TO MICHAEL F. ALTSCHUL

Question 1. I commend the work the Federal Communications Commission (FCC) and the Federal Trade Commission (FTC) have done in establishing a national Do-Not-Call Registry pursuant to their authorities under the Telephone Consumer Protection Act (TCPA). The registry is nationwide in scope, applies to all telemarketers (with the exception of certain non-profit organizations), and covers both interstate and intrastate telemarketing calls. Recently, I have heard a number of concerns from my state regarding the regulation of high volume auto-dialer initiated voice over Internet protocol (VOIP) "broadcasted" calls. My understanding is that these calls can put 10,000 calls per minute onto Indiana's landline telephone network, by using VOIP technology, in an attempt to get around Indiana's Do Not Call List. Does the technology exist to identify these high volume, auto-dialer initiated calls in real time?

Answer. Network traffic management technologies exist that can identify a high volume of calls delivered to a carrier at an interconnection point. However, robo-callers can thwart these technologies by routing calls over different paths, limiting the volume of calls presented at any one point, using a mix of messages and a mix of spoofed Caller ID addresses to disguise the common origin of these calls. Moreover, there are lawful high volume auto-dialer calls sent with the recipient's express consent (airline flight delays, school closings, etc.) and there is no technology that provides real-time identification of lawful versus unlawful high volume calls.

Question 1a. My understanding is that when phone calls are made, there are usually two user-facing identifiable pieces of information: a phone number and a Caller ID Name (CNAM). I understand that the CNAM can be used to display the calling party's name alongside the phone number, to help users easily identify a caller. I have also been told that there are numerous CNAM lookup services which allow you to pay a small fee to lookup the CNAM of a specified caller (by phone number). Do any prohibitions exist to prevent this practice by telemarketers?

Answer. I am not aware of any such prohibitions, but question whether such lookups will be useful in changing the behavior of serial robocallers, as those entities are most likely spoofing their numbers to defeat Caller ID or routing traffic to make identification of its origin difficult. See, for example, *http://800notes.com/forum/ta-19b1ccea03917e7/scammers-now-spoofing-good-phone-numbers* and *http://www.courthousenews.com/2011/08/16/39024.htm.* Additionally, the blocking of calls based on CNAM data could result in the blocking of legitimate calls.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MARK WARNER TO MATTHEW STEIN

Question 1. Over the past year or so, my office has seen a marked increase in calls and letters regarding possible abuses by some telemarketers. Since January 2013, my office has heard from more than 300 people requesting assistance with the Do Not Call List, and since taking office in 2009, my office has heard from over 1200

people on this issue. A small sampling of some of the concerns we have received are also included in this document for the record.*

As a supporter of the Do Not Call Act, I sympathize with the frustration of my constituents. I recognize that the same technology that is allowing telephone service providers to more efficiently manage networks is also enabling disreputable callers to abuse the system.

Still, it seems to me that if we can't find a technical solution to abusive telemarketing calls, that raises many serious questions as well. I encourage you to think more creatively about possible solutions, and about any legislative authorities that would better enable the FTC to keep pace with technology. For instance, have similar problems occurred in other countries? If so, are there any solutions adopted in other markets that might be applicable in the U.S.?

Answer. Primus Canada confirms that issues related to mass unsolicited calling, including abusive telemarketing calls (together, "telemarketing"), are not unique to the U.S. and are of a similar significant concern to its customers in Canada. In response to these concerns, Primus Canada invented, developed and deployed a patented technological solution called Telemarketing Guard to assist its customers with this issue.

Telemarketing Guard provides customers with control over how they wish to deal with telemarketing calls. When a Primus Canada customer receives a call identified

---

* Selected Constituent Robocall Concerns

"It is an invasion of our privacy, and it ties up our phones and disrupts our lives to get as many as 15 calls every single day when we have been on the donotcall list since day 1. Anything you can do about this issue will be greatly appreciated."

—Constituent from Arlington, VA 5/26/2012

"I am registered on the "Do Not Call" list for my home phone (not cellphone) and I am still getting many solicitation "robo calls" for lower credit card rates, car warranties, and other commercial products. Some callers block caller ID. I systematically report these callers via the "report a violator" process on the Registry website. I have been on the do-not-call registry since its inception, and I have verified this on the Registry site. I also put my elderly mother's home phone number on the DNC Registry several years ago. She also gets many solicitation calls. I am well versed on the types of calls that the DNC system is supposed to address, and the kinds of calls that are excepted. I am astonished at the number of calls I am getting even as I am on the DNC list."

—Constituent from Fairfax, VA 05/04/2012

"xxx-xxx-xxxx [redacted]. This number continues to call with impunity, even though they are on my FTC Do Not Call Registry, and several other residents I'm friends with. They are scam artists, trying to mine personal information, and the FTC hasn't responded to my concerns. Are you game for going after this group of obvious scammers, because a lot of vulnerable citizens, could be prey for their scam which involves lowering debt. They call themselves [redacted], and they are a company I and others have never done business with. Thank you kindly."

—Constituent from Fairfax, VA 06/06/2012

"I have been getting calls on my home phone from a 'Credit Card Services' for over a year now. I have submitted at least five complaints on the FTC website and at least two complaints' on the 'Do Not Call' website. I have asked to speak to a supervisor numerous times, only to be hung up on. I have told them over and over and over again to not call me. I have threatened them with FTC complaints. I have received over 30 calls from this company and have turned in many complaints to the Federal Trade Commission and nothing seems to work. If you look on the internet, you will see tens of thousands of complaints. Therefore, I would like to request that you (my congressmen) get the Federal Trade Commission to do their job and shut these people down."

—Constituent from Alexandria, VA 07/23/2012

"Over the last couple of months, I've been getting an increasing number of robo-dialer/recorded commercial calls in violation of the Do-Not-Call registry. Many have been from the same 'crook', often "Credit Card Services." I've reported most of them on the FTC's Do Not Call registry. (That is not counting the growing number of political calls, which unfortunately are not violations of Do Not Call)."

—Constituent from Reston, VA 08/20/2012

"Senator—Please have someone on your staff Google (xxx)xxx-xxxx [redacted] and you will see several websites dedicated to complaints about harassing phone calls from this number asking if we want to refinance our VA loan. We have been on the Do Not Call list since 2006 and have asked them to stop calling us 6–8 times a day. They pointedly refuse to stop. This is not about freedom of speech, it is invasion of privacy. I, on behalf of many, many people request my Federal Government figure a way to make these people stop calling over and over again."

—Constituent from Yorktown, VA 08/27/2012

"My name is [redacted] and I reside in Charlottesville, VA. I am in the fourth grade. I am writing to ask that you help by intervening in the issue of unsolicited phone calls. Our number is on the Do Not Call list. In the last two days we've received three such calls."

—Constituent from Charlottesville, VA 05/23/2012

as a telemarketing call by the Telemarketing Guard system, the call is impeded and does not go directly to the customer. Instead, a message is played advising that the customer does not accept telemarketing calls and invites the caller to announce themselves. The customer then has the choice to accept the call, refuse the call or send the call to voice-mail.

Importantly, Telemarketing Guard uses the actions of customers to identify potential unsolicited telemarketing calls. When a customer receives an unscreened telemarketing call, the customer is able to report the call to the Telemarketing Guard system. When a threshold of customers reporting the same number is reached, the system begins to monitor the calling phone number and applies a number of behavioral characteristics (*e.g.,* frequency of calling, time of day concentration, sequential calling, etc.) to determine whether the call should be identified as a telemarketing call on a going forward basis. In essence, the system promotes and relies on customer engagement to identify potential telemarketing calls.

Notably, the response by Primus Canada's customers has been exceptional. Based on internal surveys, the service has increased customer satisfaction and become one of the leading reasons that customers choose to keep their phone service with Primus Canada.

Accordingly, Primus Canada is of the view that Telemarketing Guard represents the very type of creative solution contemplated in this Question for the Record.

Question 2. In 2012, the Federal Trade Commission (FTC) challenged innovators to come up with a solution that would block illegal commercial robocalls on landlines and mobile phones. One of the proposed solutions creates a filtering system, similar to an e-mail spam filter, that intercepts and filters out illegal robocalls using a technology that "blacklists" and "whitelists" phone numbers. The proposal envisions a consumer-facing system, however, others have suggested that a network-based system might be more efficient and less burdensome for consumers. Do you believe that a filtering system would be effective? If so, do you believe it should be implemented by networks or by consumers? If not, do you have ideas for a better solution?

Answer. As noted in response to the first Question for the Record, Primus Canada provides a service called Telemarketing Guard that enables its customers to control how they wish to address mass unsolicited calling ("telemarketing").

Telemarketing Guard service is distinct from technologies that rely on the use of blacklist and whitelists solutions ("list solutions") to intercept and filter out telemarketing calls, including illegal robocalls, as it relies on dynamic information to identify potential telemarketing calls. Specifically and as described in response to the first Question for the Record, Telemarketing Guard uses the actions of customers and the application of behavioural characteristics to determine whether a call should be identified as a telemarketing call.

Primus Canada is of the view that the use of dynamic information has a number of significant advantages relative to the reliance on the type of static information that is generally associated with administered list solutions. For example, the use of static information requires significant manual administration, oversight and intervention. This is necessitated by the fact that being placed on a blacklist has a number of significant ramifications to the calling party. As a result, a process is required to validate that a number should be blacklisted to protect against the erroneous or mischievous reporting of telephone numbers. A dispute process is also required to address claims that a number should not have been, or should no longer be, placed on the blacklist.

In comparison, the use of dynamic information by the Telemarketing Guard system alleviates these concerns. For example, concerns of erroneous or mischievous reporting are addressed as a call is identified as a potential unsolicited call only after a threshold of reports by customers is reached and behavioral characteristics are applied. Similarly, dispute processes are not required as a number will cease being identified as a potential unsolicited caller if customers stop reporting calls from that number.

As for implementation, Primus Canada views Telemarketing Guard as both a network-based and customer-facing solution. Indeed, Telemarketing Guard relies on customer provided information and engagement to identify telemarketing calls. Customers may also enable and disable the service at will, though few select the latter option. On the other hand, implementation in the network ensures that customers can benefit from the service without, for example, having to purchase equipment or software, actively participate in reporting or continually update individual lists.

For these reasons, Primus Canada has selected to implement Telemarketing Guard in its network and in a manner that relies on dynamic information to identify potential telemarketing calls.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. DAN COATS TO MATTHEW STEIN

I commend the work the Federal Communications Commission (FCC) and the Federal Trade Commission (FTC) have done in establishing a national Do-Not-Call Registry pursuant to their authorities under the Telephone Consumer Protection Act (TCPA). The registry is nationwide in scope, applies to all telemarketers (with the exception of certain non-profit organizations), and covers both interstate and intrastate telemarketing calls. Recently, I have heard a number of concerns from my state regarding the regulation of high volume auto-dialer initiated voice over Internet protocol (VOIP) "broadcasted" calls. My understanding is that these calls can put 10,000 calls per minute onto Indiana's landline telephone network, by using VOIP technology, in an attempt to get around Indiana's Do Not Call List.

Question 1. Does the technology exist to identify these high volume, auto-dialer initiated calls in real time?

Answer. Yes, the technology to identify and address high volume auto-dialer initiated calls exists. In fact, Primus Canada has invented and deployed a service since 2007 that enables its customers in Canada to address such examples of mass unsolicited calling.

Primus Canada provides a service called Telemarketing Guard to all of its telephone customers in Canada. This service enables its customers to report a received telemarketing call (including auto-dialer initiated calls) to the Telemarketing Guard system.

When a threshold of customers reporting the same number is reached, the system begins to monitor the calling phone number and applies a number of behavioral characteristics (*e.g.,* frequency of calling, time of day concentration, sequential calling, etc.) to determine whether the call should be identified as a telemarketing call on a going forward basis.

When a Primus Canada customer receives a call identified as a telemarketing call by the system, the call is impeded and does not go directly to the customer. Instead, a message is played advising that the customer does not accept telemarketing calls and invites the caller to announce themselves. The customer then has the choice to accept the call, refuse the call or send the call to voice-mail.

Accordingly, in the example put forward in the question, the auto-dialer initiated VoIP calls would be identified and impeded by the Telemarketing Guard system when the threshold of customers reporting the number is reached.

In essence, Telemarketing Guard promotes and relies on the choices and actions of Primus Canada's customers to identify unwanted telemarketing calls. If enough customers accept a call from an identified telemarketer, the number will similarly cease to be considered a telemarketing call by the Telemarketing Guard system.

Accordingly, Primus confirms that the technology exists to identify high volume, auto-dialer initiated calls.

Question 2. My understanding is that when phone calls are made, there are usually two user-facing identifiable pieces of information: a phone number and a Caller ID Name (CNAM). I understand that the CNAM can be used to display the calling party's name alongside the phone number, to help users easily identify a caller. I have also been told that there are numerous CNAM lookup services which allow you to pay a small fee to lookup the CNAM of a specified caller (by phone number). Do any prohibitions exist to prevent this practice by telemarketers?

Answer. Primus is not aware of any prohibitions that exist that prevent this practice by telemarketers.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MARK WARNER TO AARON FOSS

Question 1. Over the past year or so, my office has seen a marked increase in calls and letters regarding possible abuses by some telemarketers. Since January 2013, my office has heard from more than 300 people requesting assistance with the Do Not Call List, and since taking office in 2009, my office has heard from over 1200 people on this issue. A small sampling of some of the concerns we have received are also included in this document for the record.*

---

* Selected Constituent Robocall Concerns

"It is an invasion of our privacy, and it ties up our phones and disrupts our lives to get as many as 15 calls every single day when we have been on the donotcall list since day 1. Anything you can do about this issue will be greatly appreciated."

—Constituent from Arlington, VA 5/26/2012

As a supporter of the Do Not Call Act, I sympathize with the frustration of my constituents. I recognize that the same technology that is allowing telephone service providers to more efficiently manage networks is also enabling disreputable callers to abuse the system.

Still, it seems to me that if we can't find a technical solution to abusive telemarketing calls, that raises many serious questions as well. I encourage you to think more creatively about possible solutions, and about any legislative authorities that would better enable the FTC to keep pace with technology. For instance, have similar problems occurred in other countries? If so, are there any solutions adopted in other markets that might be applicable in the U.S.?

Answer. I am the co-winners of the FTC Robocall Challenge and I think that there most definitely are technological solutions to this problem. Many of the entries to the FTC Robocall Challenge had very creative uses of inexpensive technology. Computer processing power is getting faster and cheaper by the day. Building a system to fingerprint robocaller calling patterns is definitely within reach.

Question 2. In 2012, the Federal Trade Commission (FTC) challenged innovators to come up with a solution that would block illegal commercial robocalls on landlines and mobile phones. One of the proposed solutions creates a filtering system, similar to an e-mail spam filter, that intercepts and filters out illegal robocalls using a technology that "blacklists" and "whitelists" phone numbers. The proposal envisions a consumer-facing system, however, others have suggested that a network-based system might be more efficient and less burdensome for consumers.

Do you believe that a filtering system would be effective? If so, do you believe it should be implemented by networks or by consumers? If not, do you have ideas for a better solution?

"I am registered on the "Do Not Call" list for my home phone (not cellphone) and I am still getting many solicitation "robo calls" for lower credit card rates, car warranties, and other commercial products. Some callers block caller ID. I systematically report these callers via the "report a violator" process on the Registry website. I have been on the do-not-call registry since its inception, and I have verified this on the Registry site. I also put my elderly mother's home phone number on the DNC Registry several years ago. She also gets many solicitation calls. I am well versed on the types of calls that the DNC system is supposed to address, and the kinds of calls that are excepted. I am astonished at the number of calls I am getting even as I am on the DNC list."

—Constituent from Fairfax, VA 05/04/2012

"xxx-xxx-xxxx [redacted]. This number continues to call with impunity, even though they are on my FTC Do Not Call Registry, and several other residents I'm friends with. They are scam artists, trying to mine personal information, and the FTC hasn't responded to my concerns. Are you game for going after this group of obvious scammers, because a lot of vulnerable citizens, could be prey for their scam which involves lowering debt. They call themselves [redacted], and they are a company I and others have never done business with. Thank you kindly."

—Constituent from Fairfax, VA 06/06/2012

"I have been getting calls on my home phone from a 'Credit Card Services' for over a year now. I have submitted at least five complaints on the FTC website and at least two complaints' on the 'Do Not Call' website. I have asked to speak to a supervisor numerous times, only to be hung up on. I have told them over and over and over again to not call me. I have threatened them with FTC complaints. I have received over 30 calls from this company and have turned in many complaints to the Federal Trade Commission and nothing seems to work. If you look on the internet, you will see tens of thousands of complaints. Therefore, I would like to request that you (my congressmen) get the Federal Trade Commission to do their job and shut these people down."

—Constituent from Alexandria, VA 07/23/2012

"Over the last couple of months, I've been getting an increasing number of robo-dialer/recorded commercial calls in violation of the Do-Not-Call registry. Many have been from the same 'crook', often "Credit Card Services." I've reported most of them on the FTC's Do Not Call registry. (That is not counting the growing number of political calls, which unfortunately are not violations of Do Not Call)."

—Constituent from Reston, VA 08/20/2012

"Senator—Please have someone on your staff Google (xxx)xxx-xxxx [redacted] and you will see several websites dedicated to complaints about harassing phone calls from this number asking if we want to refinance our VA loan. We have been on the Do Not Call list since 2006 and have asked them to stop calling us 6–8 times a day. They pointedly refuse to stop. This is not about freedom of speech, it is invasion of privacy. I, on behalf of many, many people request my Federal Government figure a way to make these people stop calling over and over again."

—Constituent from Yorktown, VA 08/27/2012

"My name is [redacted] and I reside in Charlottesville, VA. I am in the fourth grade. I am writing to ask that you help by intervening in the issue of unsolicited phone calls. Our number is on the Do Not Call list. In the last two days we've received three such calls."

—Constituent from Charlottesville, VA 05/23/2012

Answer. I do believe that a filtering system would be effective in reducing the amount of robocalls that get to consumers' phones. Even simple blocking techniques would dramatically reduce the number of calls that interrupt and annoy consumers.

I believe that the solution should be jointly implemented by the networks and consumers. The carriers should offer it as an additional service, but it would have to be enabled (opt-in) by the consumer. Most enhanced services such as call waiting and call forwarding are offered this way today. Consumers should ultimately have the tools available to them to block the calls that they don't want to receive.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. DAN COATS TO AARON FOSS

I commend the work the Federal Communications Commission (FCC) and the Federal Trade Commission (FTC) have done in establishing a national Do-Not-Call Registry pursuant to their authorities under the Telephone Consumer Protection Act (TCPA). The registry is nationwide in scope, applies to all telemarketers (with the exception of certain non-profit organizations), and covers both interstate and intrastate telemarketing calls. Recently, I have heard a number of concerns from my state regarding the regulation of high volume auto-dialer initiated voice over Internet protocol (VOIP) "broadcasted" calls. My understanding is that these calls can put 10,000 calls per minute onto Indiana's landline telephone network, by using VOIP technology, in an attempt to get around Indiana's Do Not Call List.

Question 1. Does the technology exist to identify these high volume, auto-dialer initiated calls in real time?

Answer. I think that there most definitely are technological solutions to this problem. Many of the entries to the FTC Robocall Challenge had very creative uses of inexpensive technology. Computer processing power is getting faster and cheaper by the day. Building a system to fingerprint robocaller calling patterns is definitely within reach.

Question 2. My understanding is that when phone calls are made, there are usually two user-facing identifiable pieces of information: a phone number and a Caller ID Name (CNAM). I understand that the CNAM can be used to display the calling party's name alongside the phone number, to help users easily identify a caller. I have also been told that there are numerous CNAM lookup services which allow you to pay a small fee to lookup the CNAM of a specified caller (by phone number). Do any prohibitions exist to prevent this practice by telemarketers?

Answer. I am aware of some companies that allow high-volume callers to display customized CNAM data however I don't know about the legality around this practice.

○