UNITED STATES OF AMERICA

FEDERAL TRADE COMMISSION

ROBOCALLS: ALL THE RAGE

AN FTC SUMMIT

Thursday, October 18, 2012

9:00 a.m. to 5:00 p.m.

United States Federal Trade Commission
Conference Center
600 New Jersey Avenue, Northwest
Washington, D.C. 20001

TABLE OF CONTENTS

Welcome:

The Network:

The Industry:

The Law:

Caller ID Spoofing And Call Authentication Technology:

Data Mining and Anomaly Detection:

Call-Blocking Technology:

Announcement:

P R O C E E D I N G S

- - - - -

WELCOME

MS. DAFFAN: We can get started now. Thank you all for your patience. I am thrilled to be kicking off this meeting today. Sorry it took us a little while to get going, but we are all very excited that you're here and that you're listening on the Webcast, if that's where you are.

I have to start off, unfortunately, with a few administrative things. For those of you who are here in person, you got a nametag when you came in. You should keep that on you at all times because that's what indicates to security that you're authorized to be here.

If you leave the building, when you come back in you'll have to go through security again, just so you know. And the other thing that we always have to say is that if there's some issue and the building is evacuated, we all go across New Jersey Avenue together to the Georgetown Law School campus and we stand there.

Okay. So the other thing is questions. Everyone who is here in the room with us, if you picked up a folder when you came in, there are little cards in there where you can write your questions. When you have a question for a particular panel member -- and all of our panels will be open to questions afterwards -- then you just hold up the card and someone will come and pick it from you and bring it up to the moderator.

You should know that this whole event is being live-Tweeted, and you can submit your questions by Tweet or by Facebook, or by email. And all the instructions for that are on the Webcast page.

So finally, without further ado, I am very excited to be introducing the chairman of the Federal Trade Commission, Jon Leibowitz. The bios for all of our speakers are in your materials. So we’re not going to spend a lot of time on introductions. But suffice it to say, the Chairman is an absolutely tireless advocate for the rights of consumers, including all of us who have received illegal robocalls. Thank you very much for being here.

CHAIRMAN LEIBOWITZ: Thank you for doing the housekeeping this morning, Kati. Let me just thank all of you for being here. It is a terrific crowd. This is the first annual FTC Summit Meeting on Robocalls. We're exceedingly glad that all of you are here, whether in person or via the web or via phone dial-in now, right? Yes.

At the FTC, we pride ourselves on the fact that we take a multi-faceted approach to consumer protection issues that includes enforcement, education, policy, and advocacy. Today's summit is a living example of what we mean. Here you are, distinguished technologists, telecommunications experts, and law enforcers, all sitting together in one room to help brainstorm on ways to stop the onslaught, and it is an onslaught, of the wave of robocalls.

Now, everyone here knows that robocalls are intrusive and disruptive because probably all of us in this room have experienced it. That's bad enough. But by deceptively pitching phony products and services such as debt reduction programs and mortgage modification scams, these bottom feeders are not only disturbing our peace, our homes and violating what Justice Louis Brandeis called our right to be let alone -- Louis Brandeis, by the way, along with Woodrow Wilson, were to be the architects of the creation of the Commission -- but they are also stealing our money.

(Whereupon, a phone rings.)

CHAIRMAN LEIBOWITZ: Who's calling?

(Whereupon, an audio was played.)

CHAIRMAN LEIBOWITZ: Does that voice sound familiar to any of you in the audience?

Raise your hands, actually, if you've got the call from Rachel. Yeah, I have too.

Well, let me tell you this Rachel, as the subject of more than 200,000 complaints to the FTC every month, it is a major source of anger and irritation across the country. You are now Public Enemy Number 1. We can't see her face, but we know she's a bad human being.

And just look at some of these tweets. Can we scroll some of the tweets? You'll understand why this summit is called Robocalls: All the Rage. I'll just read a few of them.

"There is a special place in hell for Rachel from Cardholder Services." Would I really go to jail if I found and murdered Rachel from Cardholder Services?" I'm not so sure about this because in the United States we have something called laws.

We even get old school U.S. Postal mail complaining about robocalls, and we get a lot of it. I got a letter from a man in Michigan who called robocalls, and I quote, "Malevolent predators" that are "clearly prowling among the unsuspecting for opportunities to trick them out of money." He closed his letter by asking us to, "please put your best investigators on this and protect the American people from such evil-doers." And that's exactly what we have been trying to do here at the FTC.

We sue Rachel multiple times, as well as her chipper co-workers, like Heather from Cardholder Services, Stacey from Cardholder Services. In fact, we have brought more than a dozen cases targeting either robocalls, taking action against 42 companies and 24 individuals. And we have stopped billions, literally billions of illegal robocalls.

Spoiler alert: We have more cases in the pipeline, just stay tuned for the next couple of weeks. You can look forward to continued aggressive law enforcement from the FTC, as well as from our state and federal agencies that are here today.

With that said, we know law enforcement alone can’t stop the robocalls. And that's why all of us are here today to take a deeper look. We'll start with some history. What is it about the infrastructure of the telecommunications system that has enabled the growth of illegal robocalls in such a short time?

With the experts as our guides, we'll see the technological changes that have boosted the bandwidth for VoIP, exponentially, bringing, of course, tremendous benefits to consumers. At the same time, they've been able to have voice blasting technology to flourish at bargain basement prices.

We'll talk about the dramatically growing problem of back office violations from India. You know, it has been nearly 10 years since the FTC spearheaded and implemented the National Do Not Call Registry. Today, there are more than 217 million -- 217 million phone numbers that are on the registry today. And there is no question that our efforts have significantly reduced the number of unwanted telemarketing calls people are getting from legitimate marketers who honor the system and recognize the importance of respecting consumer choice.

We also know how much American consumers value the Do Not Call system, as well as how much is valued by Dave Barry, the American humorist who called Do Not Call the most effective government program since the Elvis stamp. I'm not going to laugh at my jokes.

But let’s be honest, the telecommunications infrastructure, like so many other core ecosystems, was not developed with an eye towards fighting crime. Alexander Graham Bell did not especially focus on telemarketing fraud, let alone caller ID spoofing, when he invented the phone. Still, we are sure the technology, used creatively and thoughtfully, can help us stem the tide of telemarketing abuse and misuse.

Today's agenda is ambitious. It is engaging and it is provocative. Robocallers are becoming increasingly creative in perpetuating their scams and we need your help; that is, the help of everyone here in the room today, to develop creative solutions to catch and outwit the perpetrators.

Nothing, nothing is off the table. Technological approaches to locate and shut down boiler rooms, tougher penalties and jail time, creative ideas from the public at large, and there will be more on that with a special announcement later today. Really, anything that will help us retain our peace and quiet in our homes.

So thank you all for attending. Now I have the honor of introducing our first two panelists, who are both equally distinguished, yet eerily similar. Why don't you guys come on up. I'll explain it.

First, let me introduce the FTC's new Chief Technologist, Steve Bellovin. He joins us on leave from Columbia University, where he is a sought-after professor of computer science. Steve has spent many years at AT&T Bell Laboratories doing his graduate research for both an M.S. and Ph.D. in computer science from the University of North Carolina at Chapel Hill.

Steve helped create Netnews. And if that isn't enough, Steve holds a number of patents on cryptographic and network protocols. We are incredibly grateful that you are on our side, not theirs. For these and many more reasons it has just been great to have you as our first -- as our second chief technologist for FTC.

Next, I'd like to introduce Henning Schulzrinne. I hope I pronounced it properly. The Levi Professor of Computer Science at yes, Columbia University, and the FTC's chief technologist.

Henning also worked at AT&T Bell Laboratories before joining the computer science and electrical engineering departments at Columbia University. So I think you can sense the common theme here, Columbia University and AT&T Bell Labs have really developed wonderful technologists who also are committed to public service. Branching out on his own, Henning co-developed the internet standards that are used in internet and multimedia applications, including RTP, RTSP, and SIP.

So we have here two of the foremost thinkers in public policy and government about technology. The FTC and the FCC's chief technologists working together on behalf of consumers, thinking creatively about ways to stop illegal robocalls and to track down the perpetrators.

Please join me in welcoming the first two panelists. Thank you.

(Applause.)

THE NETWORK

MR. BELLOVIN: Thanks, John. I'm going to talk about the history of the telephone system. If you go way back, you couldn’t really make very many calls or make them very quickly since every call involved interacting. Do you remember Lily Tomlin's Ernestine character? Someone was sitting there with a switch, were pulling out wires and plugging them in. You knew who was calling.

If nothing else, you traced the wire and you could probably go ask the operator, "Who was that who just called me?" You didn't have to go through elaborate mechanisms to trace back who's doing things.

You know, we even had little iPhones, at least phones in shapes of "I." But if you look closely, you notice that this is actually a pay phone, this little box off to the right where you deposited nickels when the operator told you to. It wasn’t exactly automated, but it made a sound that the operator would recognize.

Why a sound? Because the phone network carried sound, not data. So we didn’t really have sophisticated end systems and we didn't have sophisticated computing devices. This mechanical calculator was probably state-of-the-art around 1950 or so and persisted into the mid-'60s. I actually played with a very similar one when I was in high school. No electronics in there. Period. Wasn't going to make any phone calls. But even way back when there was science involved.

What you see in front of you is a picture of a so-called central office. An early central office phone -- which this particular one was built in 1923 -- if you look very carefully, down at the bottom, you'll see there really was still a few probe wires making old-fashioned manual switchboard calls, but you'll also see that even the candlestick phone there has a dial on it. We moved ahead to the dial era.

Now, the dial era goes back, actually, 25 years before the panel switch was invented and was called the Strowger switch. Rumor or legend has it that Strowger, who, as we know, was an undertaker, invented the automatic phone switch for reasons of competition. His competitors wanted the local phone operator, when someone very aggrieved called and picked up the phone, asked the operator to connect me to the undertaker. Guess who got all the business? So he sort of invented his way out of the problem, competition problem.

But also, the volume of phone calls was

getting too high for purely manual call processing. It just wasn't going to stand. So we started getting abuse even very early on. This is a pen register. Reel paper tape was an associated gadgetry, going back to the 1920s. A pen register is a device for recording what phones are calling, what phone numbers a particular phone is dialing.

Again, this is a time of dial age, back when you were dealing with manual operators. You would ask the operator, "Who just called me?" But by the 1920s when most calls were dialed, you already needed a mechanical gadget to keep track of who was calling whom. Why do you need it? Because there was already abuse going on by the 1920s.

We also saw the start of data communications. Here is a picture of a telephone. This one is vintage 1963, but the practical goes back to about the 1920s or even earlier. Keyboard apprentices started to send data bits over wires. There was also a paper tape reader that you could prepare your message offline on paper tape that loaded in and sent it much faster than any person could type.

We already see increase of speed to amplify human capabilities there. Of course, it was still sending sounds, again, because that was what the phone network could handle.

So when we look at the phone network what we see is telephone handsets, whether it's modern ones or old fashioned-candlestick phones, and a variety of different phone switches, ranging from manual switchboards to very modern electronic switching systems to complete the calls. But initially, it was a wire from every phone to the central office: one phone, one wire pair.

The central offices became automatic. We have trunks between the central offices to connect them. When you make a call, your central office contacts the receiving central office, possibly routing through intermediate switches along the way that connects you to the number you wish to call, fundamentally, though, copper wire paths between each pair of phones that's talking. Even way back when, it was more complicated than that.

Think of that, even that very manual switchboard, it could be used within an office, and, yes, it was a pair of wires from every phone in that office to the switchboard, but many fewer pairs of wires out to the phone network as a whole. So you already have lost the end-to-end relationship between one physical wire from a phone, going out to the phone network. Today we call it PBXs.

We also find evolution the way calls are set up. Way back when -- well, we have several data signaling paths and the voice path. The call setup is I want to call this number and it went along the same pairs of wires that were going to be used to handle the actual voice call.

By late 1960s, fraud was afflicting that technique and there was desire for more capabilities. So they moved the signaling path away from the voice path. A separate data network was used to set up the calls, even contacts to help board service for things like 800 number look-ups and all the other modern features that we love. You know all those lovely voice menus? Those were the phone networks of the phone company. But you're going to see a lot more complexity in there.

We also have seen tremendous change in the economics of phone system. Underwater phone cables had very limited capacity and that was true until the late '80s when the first underwater fiber was laid down. When I worked for IBM in the late '60s, to place a transatlantic phone call you had to book it in advance with the operator.

Calls were very, very expensive,

internationally. You couldn’t make them cheaply, even international. Even domestic long distance was very expensive. Many of you in the room still remember: call in the evening. The farther you call, the more expensive it is. Gee, what a great thing.

But the phone network has changed a lot. It is no longer one phone, one wire pair. We don’t have just simple paths. We have complex data flows from both the voice path and the signaling. Signaling is not the same as the voice path anymore. It's with data path, not just a voice path. Distance and location are no longer particularly important.

There's a whole separate problem of mobile phones that I haven’t even gotten into. Endpoints are no longer just phones. It’s a much more -- you know, this is not only not my grandfather's phone network; it's not even the phone network that I grew up with. It's very different. We've moved over to the Voice over IP age, which Henning will talk about.

MR. SCHULZRINNE: Are we taking questions now?

MS. DAFFAN: We'll wait.

MR. SCHULZRINNE: We'll wait. Okay. So adding on to Steve's introduction to how we got here, let me try to discuss a little bit as to what makes the problem so challenging.

As was mentioned in the introduction, there has been this tremendous decrease in cost and increase in capability in the past, I would say, 10 years. But we have seen nothing yet. Much of the telephone system that we have in our homes, if we still have landlines, are indeed, haven’t really changed all that much, but there is now movement for fundamentally, dramatically replacing the whole infrastructure to the kind of technology that Steve was alluding to.

Thus, we are at a cusp of an even more dramatic transition that we've seen. We have the technology which is now available primarily in the corporate environment and will also become the technology of choice in the consumer role.

What I want to do in the next few minutes is to go through some of the challenges that we are facing, going forward. And why some of the solutions that we might think about as obvious solutions to solve the robocalling problem are unlikely to work and we have to be far more creative.

But as I will also try to point out, because of our transition, this is a unique opportunity before the telephone system has made that transition to build in security and consumer protection into the network, going forward. So this is very opportune time to think about these issues before we have, again, a new legacy problem, except with new technology.

So briefly, I want to look at the telephone world with the eyes of a robocaller,   what has really made this opportunity so enticing. Steve already alluded to some of those aspects. I will try to go into a little bit more detail.

A reaction when I talk to people about robocalling and a slightly related problem, SMS spam, as well, various companies provide email services have at least made email spam more available. It's still a nuisance, but we can deal with it and it has decreased, if anything, in volume. Why can’t we just use the same technologies to deal with robocalls?

I'll try to address what could consumers, as individuals, do. I'll give a punch line, but unfortunately, not a whole lot. Given that, is what can we collectively, as industry, as policymakers, as technology developers do so that consumers have a fighting chance to deal with robocalls or law enforcement does as well.

Let us walk through in a little bit more detail into the ecosystem that now enables, as a combination of technologies, the modern robocall. We have now, essentially, three actors that may well be one company or one organization, or in many cases, for both technical, let’s just say law enforcement reasons. There are different entities that have created a whole economic environment to enable robocalls, selling services to each other.

So there clearly is the telemarketer themselves that actually wants to sell goods or services, however worthless they may be. Then there is an entity on the left, the qualifier, that actually picks out the marks for that particular service or advise customers to make sure that there actually are real people as opposed to machines of various sorts.

They, in turn, are fed by auto dialers that simply obtain lists of numbers, maybe just randomly dialed, or lists of particular qualifications, say seniors or others that may list people that have financial difficulties, whatever the case may be, that are then passed on to be qualified.

In particular, that allows to minimize the cost, the labor cost to the telemarketer because by the time the call reaches a live human agent, with some approximation named Rachel and you already have somebody who is not an answering machine or somebody who has already been qualified, to some extent, that they're willing to at least listen to the pitch.

Those entities then leverage the ability to access Voice over IP services. The two advantages that they offer are distance and insensitivity. You can be anywhere in particular outside the jurisdiction where you might not face prosecution and you can do that at a very low cost.

So even if the success rate of calls is very low, you still have a viable business model, which is indeed very similar to the spam model. Even if only one in a million spam messages yields a supplement sale, you still can make some money out of that. The same is not true for telephone services.

As Steve pointed out, that business model just didn't work if you had to pay a few dollars, even for the initial few seconds of the call. And in particular, as I will try to explain in more detail shortly, VoIP makes it much easier to hide the true identity of the call and insert caller identity information of somebody else, either to obscure your origin with no particular intent to hide behind somebody else simply for all calls to appear to come from different numbers so that you cannot block those easily.

Or even more nefariously, pretend to be an organization that you trust, such as a bank, a government agency, Social Security Administration, a doctor's office, or other entity where the call person is more likely to both pick up the phone and believe, at least initially, the sales pitch.

Then these variety of telephone carriers that often have a very tenuous relationship with each other in the sense that the first one may not know who the last one is through various schemes, such as leased call routing. That is currently used where there is a much more complicated business relationship between entities, compared to what it used to be 10 or 20 years ago when you had a local exchange carrier, a long distance carrier, and another local exchange carrier and all of those carriers were Fortune 100 companies and were well known. Now you have thousands of small companies all over the world.

Indeed, the ability to distribute the infrastructure now allows these entities to be virtually anywhere. There are no special language skills necessary to do that. The technology is universal and uniform and standardized. So essentially, anywhere you can have internet connectivity, you can, indeed, build up a viable business, providing services to other parts of the robocall infrastructure.

Again, this is not surprisingly similar to what we've seen in email where we all know that certain countries seem to have a major export item in lost inheritances and bank accounts.

Let’s look at the transition. Let’s look at the call flow that we have in more detail. So we have a generated lead list that provides information, as well as there is money flow shown here on this graphic. So we have a number of suppliers and components: the lead list and the sale voice recording services so that they can be used to record responses.

You don’t know that you need until very late in the marketing game that you need a live person, so you get somebody who sounds traditionally similar to one. You need a provider of spoofed caller IDs. That is, has access to numbers and the ability to identify numbers that are not likely to be blocked.

You also have an interesting component here that most of us are not familiar with, namely, the entity or number of database providers that map telephone numbers to names which is called CNAM providers. That is, a number of database providers that at some point take a 10-digit telephone number in the U.S. and provide the name, typically provided by the customer to other entities in the chain.

They also have a money relationship in the sense that they get paid for that service. This, by the way, has all kinds of other fraud potential. For example, that database can be used to uncloak numbers who do not wish to reveal his or her identity.

And finally, the consumer's phone carrier receives the call, often unwittingly, but they do have somewhat of a financial incentive because they are often paid for terminating those calls.

In summary, we have three key components that make robocalling particularly attractive now and increasingly so; normally with cheap transport in switching, the ability to spoof numbers, and because of the ability to move internationally, to use cheap labor where labor is necessary. Much of it, obviously, can be automated. Those three things are what make robocalling much more scalable then the old boiler room ever was.

There is also a law enforcement problem. I'm not quite sure this is the best analogy, but you can think of a relative distribution of capability between the bad guys and the sheriff in town as one between the one who has a printing press and stamp out illegal materials and the sheriff who has to issue and fax individual subpoenas one carrier at a time, laboriously and manually tracing back the call to some origin in a place that they may not reach.

Here, currently, this is not just a consumer problem, but it is also a law enforcement problem in the sense that the automation has been all on the side of the bad guys. And law enforcement, because of necessity and history and lack of coordination, in some cases, operate in the analog world, often literally. That also makes it much more difficult to put a stop to it.

An important facet that has changed that makes the problem much harder, both from the consumer perspective and a law enforcement perspective, is that in the old world, as Steve pointed out, you had one device, one number and there was just no way that the customer could even change what that number was. There was no setting at the bottom of that black telephone where you could set your own number.

There was a small number of physically present local exchange carriers that had facilities that you could identify. In the Voice over IP world, you have programmable devices that could set their own number. You have a number of entities that essentially blurred the distinction between customer equipment, as

Steve mentioned, Private Branch Exchange, PBXs, and public switches. They are now essentially the same software. So that a carrier can no longer know whether somebody is a customer who is only entitled to use a small number of assigned telephone numbers or is a wholesaler that actually serves a number of other providers and can obviously transport any number.

So you only need one bad apple or one company that is less than interested in resolving these issues and you have a problem that nobody down the chain can know whether this is a legitimate call number or not.

Let's look at email for a moment. We've had, and still to some extent, a spam problem and, indeed, the vast majority of email that you never see, indeed, still spam. But we have at least used a number of techniques to greatly reduce the amount of spam that reaches consumers.

We have, unfortunately, many of these techniques are currently not applicable to robocalls. While some of those provides lessons, others, unfortunately, not quite as extensible to that space.

The name space that we have for email is essentially infinite. You can have any name, any combination. So guessing email addresses is much harder, compared to phone numbers where there is a fairly small supply. You can, indeed, dial every single phone number in the U.S. You can’t dial every possible email address; you generally have to find it somewhere that it is public. That protects a fair number of people that don't have publically available email addresses.

Particularly important is that an email, most of the spam filters inspect content and look for telltale signs, maybe combinations of inheritance, money, account number, and who knows what else, and various body parts that one might want to extend. That is less possible in phone calls.

We don’t want somebody to monitor our calls and, indeed, it would not really be possible because by the time the call has reached you, most of the damage -- in terms of my dinner being interrupted -- has already been done, so content inspection is not a viable option.

We have an email, two addresses that we can use for filtering. The network layer address, the IP address, and the email address. The email address is just like the telephone number, relatively easily spoofable. It has become harder now, but it is still something that bad actors can spoof.

The IP address, however, at least one of the delivery vehicle along the path is not spoofable because you need to be able to send the return packet back to that address. So many of the more successful techniques to block an email spam based on IP address filtering, which allows you to exclude entities that are never supposed to email to begin with.

Phone numbers, as I said, are relatively easily spoofable now and you don’t have that luxury. The delivery that we have in email is filtered by all kinds of providers. Your email provider as well as possibly third parties. You have the black list. You have spam blockers. You have standards. I guess PF and DCAM, which provide some level of attribution of email addresses, to choose certain origins.

However, in the phone world we have, and for very good reasons, the opposite. There is a strong preference, to put it mildly, that if you get a phone call, you better deliver it, regardless of whether you have suspicion that it may not actually be a desired call by the recipient. You can’t block phone calls intentionally. That would get you into deep trouble with my agency.

We have delivery traces in email. They're not always completely true, but can be partially fake, but at least the good guy part of the path, we know where the email came from. That option helps in identifying sources of email.

In phone calls, currently, tracing back calls provided by a provider is essentially manual, which makes it not scalable. We can automate-dial on a number of calls to see where they are coming from. We can do that for Voice over IP calls, but that's only something we're starting to do. Unfortunately, with technology and border control, it was often obscure about it.

In email, we have limited-use addresses. You can give addresses out to certain individuals that you’d rather not be stamped and you can make up addresses. For example, many providers allow you to claim addresses, your name, plus some tag that only you know and you only give out to certain individuals, and that a) tells you that this is somebody that you personally contacted and, b) that if somebody unwanted used that address, you know where it leaked. You know which mailing list or which webpage got that number to somebody you didn’t want to. That's certainly currently not feasible.

We can, in email -- although that has its own issue -- use a consent-based system and capture a type of system where you have to type in some scribbly things on the screen to show proof that you're human. That's really not feasible in the telephone system, at least as currently constituted.

What can consumers do? Unfortunately -- and I won’t walk you through all of these options. You can do that easily for your own amusement, but there's not much you can do because the basic problem is you don't know where the call really came from. It will always come from a different telephone number the next time same Rachel calls. If you press whatever button they offer to actually get out of it, what it means really is you've just qualified yourself even more so for the next call.

About the only viable option that you do have and the consumers do have is to file a complaint with donotcall.gov because that at least provides more data and more input to law enforcement and other mechanisms that might have problems.

What can we do in the future going forward? As I said, we are part of a major transition. Many of us have worked in the industry, essentially, replacing vestiges of the existing analog and circuit switch system with an all IP public switch telephone number.

The first thing we need -- and we'll get into that later during the day -- is trustable phone number. We simply have to have the ability, when I get a phone number, that I have to know whether that number is verified or not.

Indeed, if you go back on the web, initially, eCommerce could only take off what you had, web pages that were encrypted and authenticated, either by lock or green in bar indication. They're not perfect, but certainly we would have an even larger problem today if we didn’t have those cryptographic validations.

Both black lists and white lists, depending on trustable numbers, as well as the ability of third parties that I, as a consumer, trust to filter calls, relies on a trusted number because otherwise, everybody and anybody can just use numbers that I likely will have to include and accidently block important phone calls.

We can do that. And I won't go through the technical aspects here, but the mechanisms are there for tracing calls in the Voice over IP environment, much better than they are in the existing legacy circuit switch environment where basically you don’t have visibility into a network beyond your previous hub that delivered the call to you as a provider. Now we can actually do that.

We can trace, if we encourage and enforce that, the ability to get calls all the way back to your original Voice over IP. And, indeed, one could envision automating the process of legally obtaining trace-back information for authorized -- with an authorized subpoena that is essentially routed back to the call origin, all automatic with cryptographic validation. That would even the scales between the bad guys that automate and the law enforcement that is operating in a manual capacity.

Let me conclude that we have a situation that VoIP currently gives all of the advantages that the consumers enjoy to mainly low cost and distance insensitivity, programmable features, all to help robocallers possibly even more so.

We currently have, unfortunately, very limited consumer remedies because of the limited vantage point that consumers have and the information that they have doesn’t really allow them to block or deal with numbers that robocallers dial from.

We have difficulties in law enforcement because we are operating in a manual law enforcement world, but targets that move, that shift around, using ever-shifting set of characters and suppliers and are often transnational. Thus, going forward, I believe we need to address both facets.

We need to have a much better ability of all parties, providers, third parties that provide consumer-oriented services, as well as the consumers themselves to have access to trustable telephone numbers and we need to have the ability of law enforcement with much less effort to reach back to the entities that actually perpetrate robocalls.

MS. DAFFAN: So we can take questions now. If you have questions here in the audience, you can raise up your little card. Questions from the internet should be coming up to me.

The first question is focusing on what gives you hope that we can deal with this illegal robocall situation. And a subset of that is that some consumers trust their landlines and are sticking with them for right now. So I was wondering, is there anything that gives you hope that we can find a solution that will work for those people in shorter term while also thinking about these security by design issues that you mentioned?

MR. BELLOVIN: I'll start with the second part of this with people wanting to stick with landlines. No one is going to flash cut the phone system overnight from today's PSTN, Public Switch Telephone Network, to a pure Voice over IP packet-based network. It's going to evolve and a lot of the changes will be initially at the back end.

Your phone switch, you basically retain your landline, but your local company's phone switch will be replaced by the Voice over IP switch that's already happening, with the cryptographical authentication that Henning was talking about. To trace it back means that the caller ID display that you get will be far more reliable, far more trustworthy and then you will have far more ability to trace it back even if you don’t do anything.

As you upgrade, you can get more information delivered directly to board and have services, but a lot of the black desk telephones made in the 1920s and the 1930s still work on today's telephone networks. Remarkable. It won’t be true for tremendously much longer, but it will be true for a fair number of years more. Yeah, a lot of the change will happen where you don’t have to worry about it.

MR. SCHULZRINNE: I think in the -- first of all, I should say that whether landline or cell phone, you're just as likely to be a victim of robocalls. Unfortunately, that in and of itself, clearly does not protect you. But there is some hope beyond the items Steve mentioned in the sense that for reasons completely unrelated to robocalls, the Federal Communications Commission recently has mandated cell phone carriers to do a much better job of passing on valid signaling and numbering information.

This has to do with what’s known as intercarrier compensation and the Universal Service Fund, among other reasons, but that may well also be helpful, in some circumstances, to provide more traceable information, even in the existing system simply because many of the smaller actors, generally, for a variety of reasons -- unconnected to today's topic -- had incentives to hide the originating telephone numbers along the way, now have other reasons, beyond robocalls, to stop doing that to deliver better information, so that may help somewhere in the near term.

In the longer term, I don't think we’re talking a decade here, but we have the opportunity to do much better on the back end side of the system, but we need to tackle that quickly before there is another legacy problem.

One thing that I've learned is if you don't build that in when you have a chance, and there's always a reason -- we see that in the intercarrier compensation regime -- that you say well, we have this equipment and we can no longer change it. It’s too expensive. The manufacturer no longer exists. We can’t upgrade it. We need to do that before we get into that situation.

MS. DAFFAN: Can you say a little bit more about how we build it in? What are the steps that we can take to do that?

MR. SCHULZRINNE: So in general, I believe we need to have a -- it's a two-part problem. Right now you have no ability. The good guys have no ability to prove that they're the legitimate holders of telephone numbers. We can do that with Web addresses. Anybody here has registered a domain name with a certificate for their organization? I would suspect a few people have. It’s something that you can do commercially.

You can go to a provider with relatively little effort and you can get a registered Web address. Now, is the security level secure? It keeps out many of the bad guys in the sense of pretending to own a domain name and don't. We can't do the same thing today with telephone numbers.

We are trying to get to a model as part of a process at the FCC to see if we can get to a model where entities that are entitled to telephone numbers have a means of proving that to the upstream and downstream entities when they place a call. That requires a number of cryptographic mechanisms that are available in the protocols but have not been widely deployed at the moment. This requires industry cooperation.

MR. BELLOVIN: There are more securing mechanisms that have been designed for Voice over IP that have not yet been widely used, but it could be one reason that they will come into some use. Unlike the email, phone companies like to get paid for the service.

So if you're running a Voice over IP company, you want to make sure that you are getting paid. You know, just knowing who made a call alone is not enough unless they are trying to impersonate somebody well known, like the Social Security Administration.

I get lots of phone calls from people I've never heard of, whether it’s authentic or if this number is being spoofed, it makes no difference. It's someone I've never heard of. Yes, even from countries that seem to export bank accounts. But the phone company wants to get paid. And there are privacy-preserving cryptographic techniques that will let you trace it back, with certainty, to the originating phone company and say hey, you're responsible for this. Stop it. Much better than what you can do with email today.

MS. DAFFAN: Good. I have two questions here that deal with challenges and I'll tell you how both of them might relate to each other. One is how do you protect consumers against telemarketing robocalls while allowing automatic informational calls consumers want and need, such as school closings, fraud alerts, flight changes, package delivery?

And a different question in an era of authentication and trace-back, how do you ensure legitimate consumer and civil privacy?

MR. BELLOVIN: Well, the second part, as I said, there are cryptographic mechanisms that can be used. I don’t dare go into the details right now, but you can think of the caller's phone number as being in a sealed envelope and it’s only unsealed with the appropriate court order, possibly even using information not even known to the phone companies themselves.

Different mechanisms can be used. I have to get three different parties to agree to unseal this in order to do it. It’s not going to help with the totalitarian regime. It will help in a place where there is no illegal robocalls.

MR. SCHULZRINNE: To address the first one is actually a very important part. Unless we stop illegal robocalls, all of the desirable and necessary means of mass notification will also fall by the wayside because people will no longer pick up the phone when they don’t recognize the number, or we will end up with filtering techniques and we'll have a very difficult time distinguishing between the mass but legitimate call, such as a school closing call or other reverse 9-1-1 type of systems that have become very popular in life saving, and the Cardholder Services calls.

MR. BELLOVIN: One more point on that. In security, the way you implement authentication, like your password and your authorization, what you're allowed to do once you've proven your identity, the issue of a legitimate robocaller is authorization. They are allowed to make these calls.

You can get agencies registering with the FTC or the FCC and say I wish to be qualified to make these calls under the following set of rules, et cetera, et cetera, and they will get credentials and will say to the telephone network that they're qualified and these can be revoked if they were violating the laws or regulations. So this can be done.

MR. SCHULZRINNE: Once you can identify, you can thinking of bonding and all kinds of other techniques that we have, both from the private and the public side.

You can imagine if you have your own filtering type of service that a third party provides and they would, as has happened, have been terribly successful in some cases for email that bears legitimate mass senders who are identifiable and conform to agreed upon codes of conduct.

I can, as a consumer, can then decide which ones of those I want to do. Also, it is much easier than when I sign up for these types of services because often what I do in many cases, you know, when you think of the airline or the school district, you often sign up for these alerts ahead of time. You can then implicitly add those, despite mechanical things happening in the background, to a white list.

Even without the government dimension, there might be ways to facilitate such as white listing, as long as the parties play along and as long as you have a trustable authentication.

MS. DAFFAN: This is a question that we received in similar form from two different people. Can you elaborate as to why a consumer receives more robocalls if they press 1 or another number, to try to determine the identity of a robocaller?

MR. SCHULZRINNE: I'm guessing. Maybe there is a robocall psychologist in the room here, but my guess would be that they have found, generally speaking, something that indicates that the person is a) a real person as opposed to some answering machine or maybe an office or something. And maybe somebody who is actually naive enough to believe that it makes a difference. That may be a qualifying characteristic as well.

I don't know if anybody has published a study on why that is, but the general anticipation is that it indicates that we are much more willing to actually listen to those messages to the end as opposed to hanging up when Rachel introduces herself.

MS. DAFFAN: Great. We have a couple of questions from in the room and from email that relate very much to other panels that are coming up in the day. So I'm going to hold those questions for the moderators of those panels.

The last question is will the PowerPoint slides be made available after today? The answer to that is "Yes." All of the PowerPoint slides will be posted online, so you can have access to them. Some of those info graphics that Professor Schulzrinne used will be available for people who are in the room today.

They are outside on the table.

So with that, I'm going to turn it over to our next panel. First of all, let me just thank the chief technology officers. I will now turn it over or my colleague, Robert Anguizola, to introduce the next panel.

(Applause.)

THE INDUSTRY

MR. ANGUIZOLA: You guys can come on up. Good morning. I'm Robert Anguizola with the FTC Division of Marketing Practices. In case you don’t know, our division handles the policy work and enforcement around the Do Not Call list and the TSR provisions that prohibit illegal robocalls.

It’s my pleasure this morning to introduce our industry panel. These are representatives of the telecommunications industry that have been kind enough to share their challenges dealing with robocalls. Hopefully, they'll also be able to provide us some ideas for a path forward.

Our first panelist is Kevin Rupy. He is the senior director of policy for USTelecom. USTelecom, for those that are not familiar is the Broadband Association. It is the premier trade association representing service providers and suppliers for the telecom industry.

Next to him is David Diggs, vice president of wireless internet development for CTIA. That is the Wireless Association, and he represents the wireless communications industry.

And our third panelist is Brad Herrmann. He's founder and president of Call-Em-All. Call-Em-All is a company that offers automated dialing services. So we have someone who is actually responsible for placing some robocalls, and he is going to talk about how some are legitimate and hopefully his company is not making any of the illegal calls.

Without further ado, I present our panelists. Thank you.

MR. RUPY: Okay. Thank you, Roberto, for that introduction. Thank you, everyone, for being here today. I will just open up with a few points. I'm Kevin Rupy with USTelecom. I just want to mention four things. I want to thank the FTC for having this important panel today and we are thrilled to be a part of it.

Number two, we completely understand consumer frustration and concern on this issue. Our members are fully aware of it and they are sympathetic to it. Number three, similarly, as much as this is an issue for consumers, it's an issue for our members as well because these robocalls do, indeed, have an adverse impact on our company's networks.

Fourth and finally, USTelecom and its members have been working on addressing robocall issues through various working groups. We will continue to do so and we look forward to working with the FTC on this in the future. Three points, what I'm going to talk about today, just sort of how the network has changed; what robocalls are; and what carriers are doing to address the issue.

I don’t think that we should be surprised that on the previous panel two gentlemen who are technologists, doctorates, and former engineers with AT&T did a really great job of describing the circuit switch network.

So they covered a lot of ground and I'll sort of tee it up by talking about where we've come from and where we're going. As was discussed, the voice network has transitioned from the circuit switch voice network to a broadband-enabled voice network. This is basically what we're talking about, that sort of single-circuit connection between the consumer and the network.

I note that this slide is sort of a historic slide. Okay. It's a snapshot from say the early '90s. And there is really two things that I would like you to take away from this slide.

This circuit switch network, this original phone network was a closed system, meaning that voice services were generally provided by local exchange carriers or long distance carriers. And then when we had the passage of the '96 Act, we had the introduction of competitive local exchange carriers who are also connected to the network at both the local and long distance level, and then we brought in wireless, with the advent of mobility.

But the key point here that I want folks to take away is that it was a closed system with a very finite number of voice providers. The second thing you can take away from this slide is that at the time, these companies were providing what’s called plain old telephone service, POTS. There wasn't any internet involved in this sort of traditional, circuit switch network. But as Steven and Henning mentioned, these networks are evolving; they're changing. And what we've got now, today, is basically this, okay, we no longer have this sort of finite universe of voice providers.

We actually have a myriad of companies with diverse technical backgrounds that are providing voice services. So in addition to ILEC and CLEC and wireless, we now have Voice over Internet Protocol providers, interconnected VoIP, over the top VoIP. We have auto dialer companies. We have just this sort of vast ecosystem whereby voice services are delivered over the network. And the key thing to remember here that was raised on the last panel, the PSTN, that circuit switch network, it’s still there. It's still there. It's still out there, but it's just been kind of subsumed by the internet, if you will.

What that means is that whether a company is a circuit switch company, if you will, or an internet-based company, that voice service can transit, either through the internet or through a gateway to the PSTN. It can directly connect to the PSTN, but that voice service can get to the consumer.

I put that big auto dialer company up there just to show sort of that path. That voice path, whether it's from a web-based auto dialer company, like Call-Em-All, or it can kind of go through kind of the PSTN.

With that, when you talk about sort of the stakeholders in the robocall environment, I'm not going to go through this in great detail, but as I was talking with some folks earlier, there is a lot of stakeholders out here.

We have VoIP, we have ISPs, we have LECs, we have the robocall customers, we have the autodialer companies. And I note that there are subsets in there, okay. So even with autodialer companies, there are companies out there that just do software development.

Some manufacture equipment. Others sort of provide this bundled service to consumers, as you can see, anybody from automobile shops to zoos. But there are a lot of stakeholders in this robocall environment.

So with that, what are we talking about when we talk about robocalls? I kind of like to think about it in sort of a traffic light analogy: green, yellow, red. You know, actually, I think it's great that Brad is here today to talk about Call-Em-All because I think it's important for consumers to understand that there are a lot of legitimate companies and, in fact, robocalls that come to consumers.

So if you work from sort of left to right on this slide, reflecting all mass calling events, there are many that fall into the green category, right? And these are important and legal. And these are things like school closings, push 9-1-1 calls, weather alerts and such. You know, important calls that can be accomplished through the robocall environment or technology.

Then, of course, we have sort of in that middle area practical and legal automated calls. So these can be political messages. I'm getting called by Romney and Obama all the time now. It's that time of year. Surveys, utility call service reminders. These are practical and legal.

And then you get to the right-hand column, malicious and illegal. Phishing calls, focus nuisance attacks, people selling bogus services, these are where your bad actors fall. Please keep in mind, in all three of those categories it is not an exhaustive list. It's not an exhaustive list.

So this is sort of one important way to sort of bring all of this together, my previous slides and that last slide. We need to understand the different perspectives on these events. So there is what consumers see and there is what service providers see.

Consumers are seeing all these different types of robocalls and they understand what they're getting. Oh, my kid's school is closed. Okay. Got it. Oh, Johnny has his dentist appointment tomorrow. Can’t forget that. Rachel from Cardholder Services, right?

So they're in that position to see and understand which robocalls they're getting. Our member companies, they operate network operation centers and what they see is just a mass-calling event. They can’t delve into what specific type of call that is. All they're seeing is basically this massive spike in traffic and there are certain characteristics that are involved with these mass-calling events. They are highly localized, so they'll be to sort of a central area, say Fairfax, Virginia. They're tremendously high volume. They're extremely brief, lasting a matter of minutes, and there is absolutely no advance warning on these calls.

So basically, a massive incident over a brief period of time and then it's over and it's done. So this is an important thing to understand, sort of perspectives. Now, with that being said, I do not want to imply that our member companies are sort of passive observers to these incidents because that's simply not the case. There is a lot that they are doing when these incidents occur, and as was noted on the previous panel, there are some limitations.

Just as an example, post-event. A lot of our carriers will basically reconstruct the event and investigate. So if they receive a call from multiple consumers complaining about it, saying hey, Rachel just called me. That's an indication that, you know, we've got to look and see what we can figure out here.

So through these network operation centers they're doing things like traffic data forensics, mass-calling investigations. If the event warrants, oftentimes carriers will initiate legal actions at the federal level. That actually says state, but it's at the federal level. They work with law enforcement to pursue some of these bad actors, through the subpoena process in particular that was mentioned earlier.

Another important thing that these carriers are doing, they're working in standard setting groups and best practices groups, groups like the Alliance for Telecommunications Industry Solutions, ATIS. And these are basically where these industry stakeholders come together and figure out best practices, procedures and standards, whereby we can find consumer-centric to some of these robocall issues.

And then last but not least, there's obviously legal limitations, as was mentioned on the previous panel, in terms of interconnection obligations. Privacy plays a huge role in this. And then last but not least, there is this technological arms race component to this issue. It can be like a game of Whack-A-Mole out there.

So that is it for me. I'm happy to turn it over.

MR. DIGGS: Okay. Thank you. As noted, I'm David Diggs. I'm with CTIA. That is the Wireless Industry Trade Association, and we represent carriers, infrastructure, providers, and other suppliers. The odds are that your wireless carrier is a member of our organization.

On that note, the first presentation, there was some discussion around wireless carriers -- or carriers like to get paid. So feel free to turn your ringers up to loud because I don’t want to stand between you and our member companies and the billable event.

I do want to cover a couple of points, just two in particular. I want to point out that wireless is different from the landline environment on a couple of levels. In particular, with respect to the issue of who's allowed to call a wireless device. It's important to understand the historically, and to a certain extent, current distinction between the landline and mobile pricing regimes.

It doesn’t cost the consumer anything to answer the phone in the kitchen, but historically -- and that model is referred to calling party pays. If I want to call you at your home, then I pay the freight on that.

On the other hand, the wireless industry initially evolved with a charge for any call that you got on your wireless device. So while there were some trials of the calling party pays, in the main part, if you hit the send button or receive a call, the meter was running on that.

For that reason, the Telephone Consumer Protection Act of 1991 specifically put in provisions to forbid robocalling to mobile devices. As someone who lives in Virginia, I will second the torrent of calls to the home phone on a swing state. But I'm not getting those on my mobile device because the ethical robocalling organizations are respecting that.

There really are only those two caveats noted, emergency purposes and with the prior express consent of the call party. There is some debate about what that constitutes, but in general, it has been less of an issue for mobile customers than for landline subscribers.

And, finally, as I have already spoke to, the exemption for political or charitable does not exist for mobile.

I want to talk about, basically echoing a theme that you have already heard a couple of points on, I would speak about this in terms of the historic Telco or landline, and to a large extent, Telco and the landline operators also provide your mobile service.

The cultural differences between that and some of these new VoIP or internet service providers is that there is over a century of work that has been done in the regulatory arena with the traditional telephone companies around privacy, around CPNI, Consumer Proprietary Network Information, around PII. All of these things. And it's reached the point where it is in the DNA of these historically traditional operators to protect, at all costs, you know, the traffic that they carry from Point A to Point B. It is sacrosanct within that.

The calls are transmitted from Point A to Point B. We don't listen to them. We don't append text to them. We don't stick ads in them, et cetera. That's the sort of thing that is a key provision of the way this works.

There are innovative services that come from these new innovators, the VoIP and other internet service providers that say well, wait a minute; maybe there's a different way to do this. There is probably a market for something where if I can get the service for free, I would be willing to -- I'd be tolerant of some other services that are mixed in there.

There are services that will inspect the traffic, be that voice or text, and serve ads against that. That's fine. The difference and the problem that we're struggling with in some regard is all right, but it looks like a duck and it quacks like a duck.

It has a phone number that looks familiar to me, but there's something different going on here. How do we notify consumers that this is not your father's telephone call? That this could be something different. How do we draw those distinctions in something that looks completely the same?

The other issue -- and you've heard this alluded to as well -- in the past, there was a trusted closed network of those who could provide telephone services. That's no longer the case. You get into this sort of six degrees of Kevin Bacon game with finding out that this is a CLEC that they resold the number to someone else who, in turn, is selling to a third party, your three or four degrees of separation. And the mystery to the traditional operators has been I don't know who I'm trading traffic with. This is not at the consumer-to-consumer level, this is the operator-to-operator.

As far as I can tell, competing solutions for identifying who is, if you will, the owner of that telephone number. We talked about that earlier that there is, in fact, a finite list of telephone numbers in the U.S. It's the North American numbering plan, 10 digits; you're all familiar with them. So that is a finite universe and that is administered by an incredibly complex -- I'm not going to talk to this slide other than to put it up here and say that we spent about a half an hour on what the dotted dashed line meant in this thing. This is the North American Numbering Council, the North American Portability, Number Portability, et cetera, et cetera.

Again, that is just there to illustrate that it is a very complex question as to who it is that can draw down phone numbers and how those are identified. I'm going to go backwards here. The only other point -- and you'll hear this again. I think the next speaker is going to come up here and hit this -- but it used be that it was pretty hard to provision a phone number. It used to be that you had to go through a telephone company to do that. That's no longer the case.

So a lot of the blocking technologies are ineffective with the telephone numbers because I can change it. It doesn’t cost a lot of money. I can change it. I can spoof it. So it is a potential source of pain for consumers and for the operators and the like.

I don't have anything else, so I will turn it over at this point to Brad Herrmann.

MR. HERRMANN: Good morning. My name is Brad

Herrmann. I am the founder and president of Call-Em-All. We are an automated calling company. The first thing that I want to get out of way is I, nor is anyone from my organization Rachel from Cardholder Services.

We also make very few political calls. You might be surprised to hear those two things. What I wanted to do first is just give you a few more examples, besides school closings, for what any legitimate robocalling or automated calling company does. We send out messages on behalf of soccer and football leagues that practices or games are closed because fields are closed. We certainly do school closings. I can go on for days with examples, guys.

It may be an apartment complex calling all of the residents to let them know that tomorrow the water is going to be shut off between 10:00 and noon. And these examples -- here's one with a business example. You may have a manufacturing facility with 1,000 employees working three shifts and there's a problem on the second shift and you need to notify everybody, or that organization needs to notify their employees that hey, we're starting an hour late on the third shift today. Or we're running an extra shift on Saturday. If you want to work overtime, come on in and work.

There are thousands and thousands more

examples like this. The one thing that they all have in common, I believe, is that when people get one of these messages, if you get the message that soccer games are cancelled for tomorrow, you don't usually hang that up and go, "What a terrible robocall that was." You know, I don’t even think most people even use the word "robocall" to describe that call. But as we're seeing with infrastructure, at the end of the day it's exactly the same thing. And that's why I'm here today.

I've been asked to walk through two scenarios for you. The first one I'll walk through is, you know, these big network diagrams that Henning and Kevin and Steve have walked through, what they mean to me. It's just one little block on the diagram, and thankfully it's a lot simpler. And then what do we do to stop unwanted robocalls as the endpoint where people are entering into this network. So we'll start walking through that.

The first example is what I call old school robocalling. What I want to do with each of these examples is let's consider somebody that wants to call a million or a couple of million people. In the old school robocalling scenario, it was a much more permanent structure that you had to set up.

So you were going to be investing significant amounts of capital into specialized hardware and equipment. You were then going to need -- you certainly can't just plug in a few phone lines into the back of it because that would take you weeks. So you had to order a DS3 or, you know, T1s or something like that, with a lot of ports or lines, if you will, to come in there.

Well, those take 60 to 90 days to set up and they come with multi-year contracts and $1,000-a-month commitments to use them. So it wasn't the kind of thing you just set up, you know, slam a bunch of people with a bunch of unwanted calls and then ran away. I mean, it was two -- it was something bigger than that.

What we've seen, moving forward, is this Voice over IP robocalling. What that’s done is, you know, you don’t really require special equipment. All you need is a nice, big, fat internet connection, which you can get today in a few days. This isn't like internet connection like at home, this is something bigger than that. But certainly, this is something that can be acquired in a few days.

You also see the programming skills required become a little bit easier. You're not looking for a program that's got specific hardware, you know, experience with software that’s specialized for the hardware that you're using. It becomes a little bit more generic. I think you still need to know what you're doing, but it becomes a little bit easier. And the biggest thing we've seen in the lead time goes down to days in this scenario.

And then you take a company like mine that wraps that service up into, you know, we see cloud services all the time. We all use them for many different things. We wrap it up and our clients can now use an API or web service to come in and initiate calls.

If you went down the street to any one of these universities and grab one of the young computer science guys and say hey, I want to make a million calls and you wanted a list of a million phone numbers and you wanted him to randomly generate them, he's going to say no problem. Show me the API and I can start calling these and go.

So we've watched the initial capital requirement go from something very significant and a big investment, all the way to basically nothing, as long as you can afford the permanent rates for the calls.

The software development time has gone down to hours. And that's the situation where we are today. That's what it means to, you know, someone on the end that wants to make these kinds of calls with the way that the infrastructure has evolved.

There are a few things that stay the same, though. The first is that you always have to have a way to drop the calls onto the network. At the end of the day, they have to drop on there. The other thing is that you are going to incur some cost. All of those blocks and all of these charts that we've seen are businesses that need to get their cut of it. So it hasn’t gone down to exactly free, but what has changed is the upfront capital requirements and the upfront time requirements are what has changed.

Now that this is easy, what I would like to do is tell you a little bit about what a company like mine does to try to prevent these calls from getting onto the network. What I'm showing you today is really just a subset of what we really do. I don’t want to spell it out because there are people out there, you know, these illegal guys are actually very smart and are probably out listening. So I'm going to give you a little bit of what we do.

When you look at this you'll say oh, that's kind of common sense, but it's hard work and there's a lot of programming that went in behind it. There was one point, early on, when we went through probably a 12-month cat-and-mouse game with some of these phishers that were trying to use our service to make -- in many cases, they wanted to call hundreds of thousands or millions of people. We've done a pretty good job of blocking them out.

The biggest way to block them out is we have empowered employees that listen to messages before we approve them to go out. That sounds pretty simple, but a lot of these messages are the green messages in the red light/green light scenario. They are the green examples from Kevin's slides. It's an emergency, it's a weather notice, it's a university that needs to let all their students know that there has been a shooting incident; you need to stay indoors. Something like that. And there is a lot of yellow areas too. These are messages like I walked through with you.

Our employees listen to them and quite frankly, I tell my employees that the underlying thing is that we call people who want to be called. You can tell just by listening to one of these messages whether it sounds just fine or not. If it's Pastor Jones and the message is, "Hi. This is Pastor Jones. I'm just reminding everybody that we have three services this

Easter Sunday at 9:00, 10:00, and 11:00, instead of our normal services at 8:30 and 9:30." Okay. That's pretty easy, guys. That's no problem because he's obviously calling his congregation.

There is a lot more in the red category. What we find in the red -- actually, I categorize them in two ways: 1) they are the obvious phishers -- I call it spam, but it's not spam -- but it's the obvious garbage. And we block that and get that out right away and those people stick out like a sore thumb. But we also filter out a lot of what I call this sort of unintentional unwanted robocalls. It's the small business owner that has his customers' phone numbers and he feels he has the right, because they're his customers, to call them because they've done business with him.

What we have to do is explain to him is no, you know, you can’t do that. They have to have given you written permission to receive promotional messages from you, and we're sorry. Quite frankly, they get mad at us a lot and they get upset because they're counting on us to try to draw revenue, but we block a lot of that, folks, every day. We're out there having to educate people on what you can and can't do.

So that's it. Another way is simply just asking questions. Where did you get these phone numbers from? And people either have a good answer, "Oh, this is my congregation." Or "These are all the students in my school." Or it becomes obvious.

Now, obviously, you know, Kevin's organizations and David's organizations can’t do this with their customers, but we can. So it's what we do to try to stay on the up-and-up. And then the other thing is a lot of times because you can’t spoof the caller ID -- and we do put our clients' caller ID on the calls -- because if the school is calling, nobody wants to see a message from Call-Em-All, they want to see that the school is calling -- so we call the caller ID number. And if it’s a dead end or nobody picks it up or it's garbage, it's just one more red flag that we can do to shut these people down.

With each of our clients we maintain on opt-out list. So they all have their own -- we call it Client-Specific Do Not Call List. What we can then do, the third bullet on this, is monitor opt-outs across the range of our clients.

We've got tens of thousands of clients that are using our service; therefore, we kind of have an idea of what norms are. We can watch, when we make a broadcast on behalf of a client, if they have a higher than norm, an outlier, in terms of the number of people that opt out. That's a red flag to us that says go in and look at what this client is doing. Why are these people rejecting it? And let’s get that traffic off of our service.

That's sort of some highlights of what we're doing, among other things, to try and keep these robocalls off your cell phones and your home phones. When I'm talking about this, I'm just one organization and this is just my viewpoint and what we've done, but you have to remember that I think the biggest violators -- and I would assume that Rachel from Cardholder Services is not coming through a company like mine.

These are people that really don't care about the laws and they're willing to do, they're basically doing whatever they want to do. So we have to be careful, as we're talking about these solutions, not throw the baby out with the bathwater, if you will.

I mean, we can have all kinds of regulations. We can mandate all of these that we do to every company that we're aware of, but the fact is I don’t think that would stop Rachel from Cardholder Services because that company or that individual or organization doesn’t care to follow the laws. So that's one of the big reasons that I'm here is to try to represent the good things that are happening within this industry.

So thanks for your time. Robert?

MR. ANGUIZOLA: Thank you so much. Our first question is you posed a lot of challenges. What do you think can be done to bring down the number of bad robocalls that are barraging consumers? That’s to anybody.

MR. RUPY: I'll jump on it. I don't think there's any single solution to the issue. I think when you look at a lot of these issues that are out there today, such as robocalls, you have to look at it kind of holistically, right.

So I think one aspect of this is consumer education is critically important. I know the FTC has done a lot of great work on that. I know our member companies are doing a lot of great work on that. I think it's important for consumers to understand that while there may not be perfect rules out there, there are things they can do to limit the impact of these calls.

As an example, use of caller ID. If you don't recognize the phone number, don’t pick up the phone. Don't engage these guys. Certainly don’t press 1 or 2. I think that's important.

The last two things I'd mention to address this issue is I think targeted enforcement against some of these bad actors. I think that's always a great thing, to go after these guys.

And then thirdly I think things like this, things like ATIS that our members are involved with; working collectively with all the stakeholders on this issue to try to find solutions because I think Brad is right; it's not going to go away, so we kind of have to work collectively to at least address the issue as best we can.

MR. HERRMANN: Yeah. I was excited to hear, I think it was Steven, beforehand, and Henning talk about authenticating the users on the initiation of calls. You know, that's the kind of thing, you know, I’d be the first one standing in line, hey, authenticate me. Check me out. And we want to represent ourselves as people who are doing the right things. And that's very exciting for me in that hearing the future of technology and where things are going.

As far as individuals go, an individual consumer is hearing from me saying, oh, we're maintaining Client-Specific Do Not Call Lists. And another thing is you’re hearing advice not to opt-out, just to hang up. I think I would educate a consumer to do what I would do and listen. If it isn’t obvious, ridiculous -- if it’s Rachel from Cardholder Services, that is ridiculous. Hang up on it immediately.

If it's your school calling and you check your email every five minutes or you'd rather go to the website and you don't want them to call you, opt out. No problem.

So you kind of have to use a little bit of intuition on these calls to determine whether this is a legitimate call that you just care not to receive, in which case go ahead and opt out. If it’s obvious garbage, just hang up.

MR. DIGGS: I must be the only guy in the room who has not yet gotten a call from Rachel.

MR. HERRMANN: Do you have a cell phone?

MR. DIGGS: Yes. Well, it seems like I ought to report it, I suppose. I, too, in the earlier discussion about -- some of the solution will come in the technological form of a non-reputable, fully authenticated identifier. I mentioned in my portion of this that part of the challenge is identifying, as an operator, who is sending me this traffic. And that is often difficult to determine. I will spare you, but eSPID, aSPID, SPIDs, the last SPID used.

There all sorts of -- and I'm pleased that groups like ATIS and others are working towards finding that there is a way that, as an operator, when I'm receiving traffic from some organization that if it does go rogue in some way that I have a path to go back to that operator and say you got a problem here.

MR. ANGUIZOLA: The next question comes from the audience. It's directed to the history representatives. What kind of risk is associated with the network congestion caused by robocalls?

MR. RUPY: It can be significant. In fact, where you do have these instances of mass-calling events, and in fact, whether they're legal or illegal, depending on the volume, depending on the location of where that call is taking place and time of day, whatever factors, that they can have an adverse impact on the network, such that a consumer in that area who may be trying to make a call is unable to complete the call because network capacity is sort of maxed out. It can be a significant factor.

And in fact, there are times where, due to a mass-calling event some of our carriers may actually have to file with the FCC saying, hey, we experienced a network event here. There's a problem, et cetera, et cetera.

MR. HERRMANN: Yeah. I think there is

network blockage, that that is blocking the robocaller, too. These guys are not dopes. So I think they will figure out a gating rate on their calls that will keep their traffic at or below some threshold that would be problematic for them to continue to make the calls.

They can distribute, again, the internet being everyone. They can drop that down to any number of switches in the network. I suspect that because that's a problem for them, as well as for the consumers, that that is something that they seek to mitigate as well. We have not, even though -- the size of the wireless pipe, as it were relative to that wire line pipe is a fraction.

So we, as an industry, are always very, very concerned about bandwidth with respect to those kinds of issues, but it is something that has not been a particular plague on the wireless end.

MR. ANGUIZOLA: The next question from a listener online. They want you to speak about the economics and the money associated with robocalling and specifically what CNAM and dip fees are and how industry players can make money that way.

MR. RUPY: Yeah. There are obviously a lot of different ways that these robocallers are making money, whether it's through scamming, through the sale of bogus services and whatnot. I think what the question was referencing there, CNAM, also referred to as LIDB, which is Line Identification Database.

Basically, the way that works is that carriers will maintain a database for caller ID numbers and when a phone number gets called, that caller identification number gets pushed to the person receiving the call. That's why when a call comes to your house you see the caller ID number.

Whoever is maintaining that database gets paid for pushing that call to the recipient and the network operator basically pays that fee. It's 700th of a cent, but when you multiply that times tens of thousands of millions of calls, it can add up. So I think that's what they're referring to. You know, it's one of many ways that these guys are making money.

MR. ANGUIZOLA: Anybody else want to add to it?

So the next question takes us from profits to penalties. Should there be higher penalties for illegal robocalls, and is there some way that we can increase the cost of engaging illegal robocalling?

MR. HERRMANN: I can speak to that. The penalties, in a lot of cases with the FCC's TCPA Act, are $500 per incident and $1,500 for an intentional robocall to someone who shouldn't receive one. I think those are sufficient enough.

I've seen cases and experienced cases where one phone call led to a class action lawsuit that cost hundreds of thousands of dollars to defend, only at the end of the day to be disregarded and settled for pennies.

So I think, as an autodialer, I assure you that we are -- when I tell you that my employees are -- if you have any doubt, throw it out because the numbers are massive. I mean, if you think about $500 per phone call and let’s say we call 10,000 people in a school district, that number becomes, I think, kind of silly.

I think the penalties are there and actually, in some cases, allowing class actions to be filed on the basis of a single phone call are --

MR. DIGGS: Ridiculous.

MR. HERRMANN: -- a little much.

MR. RUPY: I would just add, I think those penalties are pretty stiff. You can ask a question about, well, is there an effort to amp up the enforcement of TCPA violations. I think that would be desirable in everyone's case.

MR. ANGUIZOLA: I think we can arrange for that. The next question is directed to Call-Em-All.

As part of your compliance process, do you keep a black list of the red operators so that they can be recognized so that you don't have to deal with them in the future?

MR. HERRMANN: Yes, we do. But the problem is, you know, how are they authenticating themselves with us with an email address, right? So we make them activate by clicking on an email address. But those, as we've already talked about, it takes anybody in this room three minutes to set up a new email address to use for this kind of stuff.

So it's very, very challenging, and there are several other things that they do that indicate to us, sort of other red flags that, like I said, I really don’t care to go into because I don't want to tell them how to beat us. But we do everything. We spend a lot of engineering time putting things in place. We have a black list of emails not to use and things of that nature.

MR. ANGUIZOLA: The rest of the questions that I've got are better directed to our law enforcement panel. So do we have any other questions?

UNIDENTIFIED SPEAKER: You know, I couldn't get in this room today without a driver's license and going through a metal detector. I'm just curious of why your clients, your customers, you're verifying their identity with an email address that can be set up in three minutes.

MR. HERRMANN: So the question was, you know, when we have driver's licenses and other things, like just to get in the room here, how do we verify our clients based on an email address only.

When they sign up with us there is far more than an email address that they provide. All of that, you know, they give us a physical address. They're going to have to give us a credit card. So we have, as well as their name, we look at all of those things as a whole and listen to their messages.

You're looking at their -- I don't want to say body of work -- but you're looking at all of it. We have screens set up for my staff to use that show you all of this at once and they are looking at it, you know, they're all college-educated folks looking at it. It paints a bigger picture than just email addresses. So my last answer might not have been clear enough to kind of paint the picture for what we're really doing to identify these folks.

MR. ANGUIZOLA: Okay. Thank you very much. It's now time for our first break.

(Brief recess.)

THE LAW

MS. GREISMAN: If everyone will take a seat, we’ll get started. Good morning. My name is Lois Greisman. I’m with the Federal Trade Commission’s Division of Marketing Practices. It’s my honor to moderate the second panel of the morning. It's on law enforcement. There are some questions about law enforcement that already have arisen, by no surprise whatsoever.

We have a very distinguished set of panelists. My intros will be brief since you all have bios. To my immediate left is Greg Zoeller, the Attorney General from the state of Indiana, well known as a compassionate consumer advocate.

To his immediate left is Will Maxson, the FTC’s Do Not Call program manager and in his free time, is a staff attorney in the Division of Marketing Practices. To his left is Eric Bash, whom I will refer to as an FTC recidivist. He has been in and out of the Agency a couple of times. Now he is associate chief at the FCC’s Enforcement Bureau.

We are going to do a slightly different format for this panel. What I am going to do is ask a series of questions and ask each of our panelists to respond to them. I’ll even preview for you exactly where we’re going to go and where we’ll spend most of our time.

What we want to do is just lay out the nuts and bolts. What is the state of the law? What are the legal parameters in which robocallers, legitimate and illegitimate, operate under?

And then after talking about that, we’ll talk a little bit about complaints, what we see in that front. Then we’re going to really spend the bulk of our time talking about the enforcement challenges and what it is we can do about them.

So let me start off and ask Will to really kick us off and lay out what are the legal parameters that we operate with.

MR. MAXSON: Good morning, everyone. So I’m just going to talk for just a minute about what the Telemarketing Sales Rule says about Do Not Call rules and robocall rules. Telemarketing Sales Rules is a rule that we enforce, and then when Mr. Bash speaks, he will talk about some TCPA, and the FCC, of course, because there’s a lot of overlap.

There are three basic protections in the telemarketing sales rule that are related, but a little bit different. The first one is the National Do Not Call, which dates back to 2003, and it’s what everyone generally thinks of, I think, when they think of the Do Not Call. Generally speaking, businesses can’t make sales calls to consumers whose phone numbers are on the National Do Not Call Registry.

As you heard, there are over 200 million phone numbers on the Registry. Those include cell phones and home phones. Any phone could be registered, as many phones as you have. When businesses make sales calls to those numbers, generally speaking, those violate our Do Not Call Rule.

There is also an entity-specific portion of the Rule. So even if your number is not on the Do Not Call List, you can ask a company not to call you again. If they do and they make another sales call to you, that violates the entity-specific portion of our list. That is true even if you have -- they’re called established-business relationship. So even if you’ve bought something from a company in the last few months and they try to call you again, under that exception to the general rule, you can tell them don’t call me again. If they do, that would be a violation of our entity-specific rule.

The third part of that is the Robocall rule, which is, generally speaking, business can’t make sales-based robocalls to consumers. Those calls are prohibited even if your phone number is not on the National Do Not Call Registry. The only exception, which I’ll talk about in just a second, is if the consumer has provided a business with expressed written permission to robocalling.

There are a handful of types of calls that are not covered under the Telemarketing Sales Rule. Business-to-business calls are generally not covered. Debt collection calls are generally not covered. Customer service and customer satisfaction calls, survey calls, only if they don’t contain a sales pitch. If it’s a survey call and it ends up trying to sell you a trip or cruise or some sort of product, then that’s covered. That’s against the rules.

Political calls are not covered under the Telemarketing Sales Rule, again if they don’t include a sales pitch. There are some special exceptions to FTC jurisdiction and those types of calls are not covered, banks, phone companies, insurance companies. There is also a separate extension for robocalls that deliver a healthcare message made by or on behalf of a covered entity as defined by the HIPAA Privacy Rule.

So what calls are covered? It's a vast majority of calls. Calls that are part of a campaign or plan to get consumers to purchase a product or service is the most general way to say it. So if there is any part of that call that is designed to end up with a consumer purchasing something, then that call is covered under our Do Not Call Rule, our Robocall Rule, our Entity-Specific Rule.

It also includes charitable solicitation calls by for-profit fundraisers, the hybrid calls that I mentioned, the survey calls and things like that where they pitch it as a political survey or some sort of survey about whatever topics they’re interested in, and then they end it with some sort of sales pitch.

Even companies with which you have an established business relationship can’t robocall you with a sales message. The established business relationship exception does not apply to robocalls. Also, companies that assist or facilitate those that place illegal calls are also subject to liability.

This is the rule that we all hear about and we’re all here for today, the Telemarketing Sales Rule Robocall Rule. It prohibits initiating a call that delivers a prerecorded message to consumers for a sales call. If it’s the type of call that falls within the FTC’s jurisdiction, the only exception is if they have written permission from the consumer, if that specific seller -- and as you see here, there are several requirements for what that written permission has to obtain. It has to be under clear and conspicuous disclosure by the seller when the purpose is to authorize the seller to place prerecorded calls.

It has to show the consumer’s willingness to receive calls, delivering prerecorded messages by or on behalf of the specific seller. It can’t be a general “I’m agreeing to get robocalls from anybody” and then some lead generator sells it to lots of different telemarketers and they all end up calling. That doesn’t count.

It can't be required as a condition of purchase, and that written exception has to -- excuse me -- that written permission has to include the consumer’s telephone number and signature. If they don’t have all of this, it’s illegal.

MS. GREISMAN: Thanks, Will. Eric, do you want to pick on the FCC’s viewpoint?

MR. BASH: Yes. So just to start at the beginning, the source of the FCC’s rules in this area come from the Telephone Consumer Protection Act of 1991, which you’ve heard people refer to this morning, and then the FCC had adopted implementing rules, you know, not long after that statute was enacted, and the rules have changed somewhat over time in the last --

what is that -- 20 years.

In some cases, including the most recent changes that have been adopted, I think just after Valentine’s Day, those were designed to harmonize the FCC’s rules as quickly as possible to the FTC’s rules. I’ll get to some specifics in a minute.

One thing to highlight for you at the beginning, though, is you heard Will mention that certain entities are not subject to the Federal Trade Commission’s Telemarketing Sales Rule largely because the jurisdiction of the Federal Trade Commission under the TSR, the Telemarketing Act, is coincident with its jurisdiction under the Federal Trade Commission Act. The FCC’s rules are not limited in that way. So some of the exceptions that you heard Will refer to, those entities are not exempt from the FCC standards I'm about to mention.

So the general standard and prohibition that emanates from the Telephone Consumer Protection Act, which is codified in Section 227 of the Communications Act, is that there can be no autodialed or prerecorded voice calls to an emergency number or numbers that are really designed to -- are basically for emergency purposes, like a doctor’s office, law enforcement, that sort of thing.

So you can’t make these calls to emergency numbers. You can’t make these calls to guest or patient rooms in hospitals or nursing homes and that type of facility. And you cannot make these kinds of calls to mobile phone numbers or other numbers for which a consumer might be charged for having received the call. The only exception to those prescriptions that I just identified is if you are making the call for an emergency purpose or you have the prior expressed consent of the called party.

There are also restrictions on prerecorded calls to what we call residential lines. Let me state this sort of in another way. Calls can be initiated -- prerecorded calls can be initiated to residential phone lines, residential landlines, if they’re made for an emergency purpose or for a commercial purpose that does not include telemarketing.

If they’re not made for a commercial purpose, if they’re made to a person with whom a caller has an established business relationship or if they’re made by or for a tax exempt nonprofit. And for those kinds of calls to fit within the legal requirements that the FCC enforces, it’s also the case that certain disclosures have to be made to the called party, namely that the person who is initiating the call has to identify who they are at the beginning of the call and during or after the call, they have to provide an actual phone number at which they can be reached.

So just to state these requirements in a different way, to summarize the distinction between landline and mobile, again, you can’t make an autodialed or a prerecorded call to a mobile phone number unless it’s for an emergency purpose or you have the prior expressed consent of the called party.

I wanted to mention when a prerecorded political voice call would be okay because that’s something that we’ve heard people refer to this morning and when those can be okay is again, when they’re made to a residential line that can’t be made to a wireless phone number unless you have the called party’s consent and you make the required disclosures of the identity of the caller as well as the telephone number, which the called party can be reached.

You’ve heard me refer to the established business relationship exception. This is one of the things that is being changed to harmonize more with the FTC's rule that says for robocalls, that doesn’t work anymore. You have to have the prior expressed written consent of the called party in order for that to be acceptable. And as I mentioned, the FCC has adopted a rule to be consistent with that on February 5, 2012. That is not yet in effect because it’s subject to some review of the Office of Management and Budget, but when that approval comes through and after the passages are signed thereafter, that will be the governing rule and the EDR exception that I mentioned earlier will not be available.

I should also just say, to close the loop, on the legal standards that the FCC enforces with the respect to robocalls, we also have a Line Seizure Rule for business calls you are not permitted to make autodialed calls to, multiline businesses; you can’t engage two or more of those lines at the same time. That's the basic overview of the FCC's rules in the area.

MS. GREISMAN: Thank you, Eric. Mr. Zoeller?

MR. ZOELLER: Well, the state’s experience, and I’ll speak specifically about Indiana, but there’re a number of states that are pooling together on these issues. In Indiana, we never had the established business exceptions. So we’ve maintained a stronger version of the Do Not Call List.

A lot of the states did fold into the federal Do Not Call since they had the same established business exception, so it’s identical. But there are number of states that still have stronger Do Not Call statutes, so we’ve maintained a Do Not Call working group, and I’ve got Margarete Sweeney from my office who’s the chairman of that. So a lot of states still pool together on some of these issues.

So we’re very active with our National Association of Attorney General. When it comes to robocalls, Indiana has another, let’s say unique experience. We’ve banned the use of autodialers since 1988, recognizing the growing opportunities for scams. We’ve even banned the political calls, so you won’t get political calls. That’s engaged a number of legal challenges, as you might have guessed.

It has been successful up through the courts and of the Supreme Court of Indiana, successfully arguing that the rights of privacy in the home trump the political free speech to blast out tens of thousands of calls to Hoosiers. It is subject to a federal case that went up to District Court that is now in the Seventh Circuit Court of Appeals.

So I do think that there are opportunities there that Indiana and other states have shown to have stricter Do Not Call and no robocalling kind of operations.

Some of the work that we are currently doing, though, is going to again be subject to additional challenges and we look forward to many more days in court.

MS. GREISMAN: Thank you. So let’s shift gears slightly and talk about targeting. How do you identify entities that you might choose to pursue or investigate?

What do you know about what complaint volumes and trending has been? Let’s stay with the state of Indiana.

MR. ZOELLER: Let’s see, I think I’ve got a slide up here somewhere. What we've really found is since the advent of the VoIP and the cloud-based robocalls, our volume of complaints has doubled just in this past year. We’ve now gone over 17,000, just since September 30th of this year.

So, again, since we did have a much stronger statute, our state Do Not Call than the federal statute, we were blessed with really a decade of, I would say, peace and quiet. I think Hoosiers still have a greater sense of expectation when it comes to privacy in the home, particularly.

So when the VoIP and cloud-based robocalls began and Rachel was working her magic in the Hoosier state, the spike in these complaints really, there was kind of geometric growth on the complaints. Some of them really come to real shock. So I want to express the righteous indignation that I have received in letters every day. But again, I think a lot of it comes from the relative peace and quiet that we’ve received in the past. Now, they’re not used to having these calls and wonder why can’t you keep people from calling.

I think a lot of states didn’t have the same experience as Indiana. They always had a little bit of the robocalling, so they’ve kind of gotten used to it. In Indiana, it has come as quite a shock, and I’ve got 17,000 complaints that I could share that fully express the righteous indignation of my state.

I think on the breakdown of the complaints, really come in a number. The largest bulk is clearly the robocalls, but we do have complaints about text messaging, which is only 17 percent and then 33 percent, which is everything from collection calls to all the rest. But truly, it’s the robocalls that incite the most and the most passionate complaints.

Again, sharing the fact that after a long decade of peace and quiet, why can’t you in the federal government do something? It’s a pretty loud and clear message. Oh, I have a picture of some of the hand notes, one of my favorites. I’ll have to share the favorite from what I assume is a grandmotherly Hoosier writes that can’t we stop the calls because she can’t even take a nap.

MS. GREISMAN: Thank you. FCC?

MR. BASH: So let me -- and I’m sorry that I don’t have a graphic to put up on the screen in front of you, but I do have some complaint volume to report to you.

In 2010 -- and let me just say at the outset, if you go to the FCC’s website and you want to file a complaint with us about robocalls, there are a variety of forms that are available there for you. I think they’re self-explanatory that you would choose from depending upon the particular type of problem you’ve experienced, and it’s collating and looking at those different kinds of complaints that have enabled us to pull together the type of statistics that I’m about to give you.

But across complaints involving prerecorded calls to residential lines, prerecorded calls to business lines, prerecorded calls to cell phones, and text messages to cell phones, in calendar year 2010, we had about 50,000 complaints across those four topical areas. You can see the growth in the figures I’m about to give you.

In 2011, there were 86,000 complaints across those areas and thus far, in 2012, and obviously we’ve still got the balance of October and all of November and December to go through, we have received, I guess it’s through October 11th, 98,607 complaints. Twenty-two for this year thus far, 22,000 of those are complaints about prerecorded calls to residential lines, about 3,000 to business lines, 36,000 to cell phones and 37,000 to cell phones.

Let me just add a footnote to the statistics that I’ve just given you. Those don’t necessarily indicate that the law has been violated in every particular case because for example, I didn’t talk about any restriction for calls to business lines and so there may be something going on there, but there may not be. So I say that not to call the statistics into question, but I just wanted to highlight for you that those numbers don’t necessarily mean that there have been 98,607 violations of laws that we enforce that we’re aware of thus far this year.

MS. GREISMAN: Thank you. Will?

MR. MAXSON: We just released our data book on Do Not Call complaints for the last fiscal year that ended at the end of September of this year. Our complaints were up just like everyone else’s, nearly double for Do Not Call complaints. Our robocall complaints are even higher and an even larger percentage than they were the year before, not surprisingly.

If you look back over about a two-year period, the line essentially looks like this, and everyone knows if you’re getting more calls, obviously we’re getting more complaints, people are getting angry about it, and we use those complaints to find the bad guys.

So what we do when we’re targeting and trying to figure out who we’re going to go after, one of the biggest things that we consider is who can we go after to stop the most number of calls. What will have the biggest impact, who do we go after?

For instance, there is a case that recently concluded that we filed against a company called Asia Pacific. We know that company had made over two and a half billion robocalls. Two and a half billion.

There’re lots of other companies that we filed against that make lots and lots of calls like that. So that’s who we figure out when we’re looking at who we’re going to go after. We take the complaints, we get information for those complaints, and we try to figure out who will stop the most number of calls.

We talk about complaint figures. We filed 94 enforcement actions involving the Do Not Call violations. Some of those include robocalls. Some of those are just specifically do not call, but 94 enforcement actions -- those are against 271 companies and 212 individuals. Those defendants in the cases that have ended, and some of them are still ongoing, have paid more than $69 million in civil penalties and equitable monetary relief.

If you look just at robocall cases, going back to three years ago when our robocall rules went into effect in late 2009 -- FTC has filed 15 cases specifically dealing with robocallers against 42 companies and 24 individuals. Although many of those cases are still ongoing and, in fact, several were filed just recently, we’ve already collected over $5 million in civil penalties and equitable monetary relief. If you keep an eye on our press releases on our website, there’s a lot more to come.

One thing we also do because we target the people that are responsible for the most bad acts, for the most calls, in many cases we think that those people deserve some criminal punishment. Although we don’t have criminal authority, unfortunately, we refer many of those cases, the worst actors, to criminal authorities for criminal prosecution.

For instance, just a couple of weeks ago, a defendant in our Transcontinental Warranty Enforcement Action was sentenced to 16 months in prison for making illegal robocalls to pitch fraudulent auto warranty services. Other defendants in those cases were sentenced to five years in prison.

Just last month, we announced as part of our enforcement action the civil action against those defendants. We were mailing refund checks to nearly 5,000 consumers across the country who were allegedly defrauded by these calls. Some of those checks were for more than $1000.

Earlier this year, a federal judge sentenced a defendant from our Economic Relief Technology Civil Enforcement Action to more than 17 years in prison and ordered her to pay more than $1 million in restitution for making illegal robocalls to consumers. In those calls, they used names like card services and account services, the types of calls that you’ve heard about today.

So because we target those really bad actors, in many cases, those bad actors deserve jail time and in many cases, they find them.

MR. BASH: Lois, I didn’t share anything, as I should have, about what our law enforcement efforts have been. I told you about the complaints that we have, but I didn’t share with you what we have done.

So just to highlight that for you briefly again, our rules have been in effect since around 1991 and 1992. Since that time we’ve issued hundreds of citations -- and let me get back to that in a minute -- and we have instituted around 10 different penalty actions that collectively are valued at around $3.5 million, I believe is the figure.

Just to circle back to the citation for you, our authority is different than what you have heard the FTC describe and as the Indiana Attorney General what they do, we do not have the power under the Communications Act to go directly into federal court and to seek an injunction. The type of enforcement process that we use is a penalty type of process in the cases of people who aren’t carriers or broadcasters. In other words, people who don’t hold licenses from the FCC were statutorily required, as a first item of business, to issue a citation to that entity.

The point of that requirement is to alert this entity that may not typically be, you know, aware that it’s operating in a regulated space that the FCC is involved in that we have to tell them, you’re doing something that you’re not allowed to do.

Then if they do it again after having been warned, then we have the power to go ahead and start penalty proceeding and the way that works and, not to get, you know, too bogged down in the nuts and bolts of FCC enforcement, is that we would issue something called a Notice of Apparent Liability, and it comes directly from the statutory enforcement procedures that the FCC has, where we tell the alleged wrongdoer what law they have violated, when we believe they did that, and what penalty we are proposing to impose for that violation.

They have an opportunity to respond to that. We then need to consider what they have to say in response and move forward with a forfeiture order that would either go ahead and impose the forfeiture that was proposed in the Notice of Apparent Liability, or NAL, or do some reduction if there is some merit to doing that, or I suppose you could cancel it. The 10 actions that I’ve referred to are at various stages in the process, some of the NAL has been imposed, but we have not yet moved forward to a forfeiture order. In some cases, we’ve gone to the forfeiture order and in some cases, there has been a consent decree with that alleged wrongdoer to resolve the matter in its entirety.

MS. GREISMAN: Thank you. So no shortage of complaints. States are getting thousands, FCC is getting thousands, FTC is getting a couple hundred thousand each month. So I think the next question is really summarized wonderfully. I'm getting inundated by cards, thank you.

Why is Rachel still calling? I think that definitely pulls together the next topic of conversation. Why is enforcement so challenging? And let's start with FTC. Will?

MR. MAXSON: Sure. I mean, you've heard about a lot of the reasons already. We've talked about the network has changed. I guess the easiest thing to do might be to walk through the way the typical Rachel type call might happen.

So it might start, and frequently does, with we call a lead generator, sometimes a qualifier, but often it is a lead generator. It can be based anywhere in the world or anywhere in the United States. All they need is a computer and an internet connection with an autodialer company. Then the autodialer company then has a connection into group VOIP carriers into the

PST and network telephone network.

So the autodialer -- excuse me -- the lead generator is just trying to find people for these products or services, which are frequently going to be scams, these Rachel calls. The back end of it is frequently a scam. So they are just going to blast out calls to whomever.

We've heard some of these lead generators are just -- they're calling the phonebook. They are going sequentially down through numbers. They're just looking for bodies, a lot like email spam, because the costs are so much lower now. The startup costs are much lower, almost zero.

As Brad mentioned earlier, you can get dialing in a few hours now. You don't need a PBX. You don't need lots of copper lines. You don't even need a phone. You just need your computer and internet connection.

So they will send out these calls, going through an autodialer. They are just going to put them into the telephone network and they'll go out all over the country. And a very small percentage of people will end up answering and listening to the message. And the message -- it'll be like the one you may have heard earlier that the chairman received, the Rachel call. It’ll say press one if you’re interested in lowering your credit card debt, press two to go on our Do Not Call list.

And if you press one, the call then will be routed to somewhere completely different. It can go to an outsourced boiler room that might be in India or Pakistan or California or Florida. It might go back to the lead generator. It might go to the company that is actually trying to pitch this scam to you.

Frequently, you will speak to a qualifier that will ask a few questions, whether you have at least $10,000 of credit card debt, at least two credit cards, and then they might just hang up on you. They are calling with a spoofed caller ID number, and they’re not going to give you a real name. They’re going to use a name like card services or account services.

When you answer and you talk to them, you don’t know anything about them. You think you know their phone number. You think you know the name. You think you know where they are because they might call from an area code even that’s near you. In fact, they could be in Panama. They could be in India. They could be in California. They could be anywhere.

In some cases, the lead generator, they’ll just hang up on you then. They got your number, they got your name and they know that you’re someone that is interested in reducing your credit card debt, they’re going to sell that information to one, 10, 20, 30 different scammers that are all going to try to call you and pitch debt relief services.

Sometimes, you will immediately get transferred somewhere else, somewhere else in the country or somewhere else in the world. Then they are going to go in and try to sell you how you need to pay $500 or $1000 to reduce your interest rates to zero on your credit cards or some sort of other outlandish scheme that isn’t true.

Because those lead generators -- and those people can be based anywhere and they can spoof your caller ID -- that makes them much more difficult to find. They can also move extremely easily. In fact in many cases, those people don’t have any connection to you whatsoever because you’re not actually going to pay those people.

The people that you end up paying, the few that do, are the scammers that are actually pitching you this card services stuff, and those people may call you on a completely separate phone call. You may not even realize that the two are connected.

So the way that we work back to try to find the bad guys and file our enforcement actions is we do a number of different things. Usually what we do is we start out with the consumer complaints that we get because even though the caller ID is usually spoofed and it’s fake and the name they’ve given is fake, you can still tease information out of those. You can still bring all of those complaints together and look for trends. Maybe they made a mistake in one particular call. Then you can connect all of those different complaints together.

For instance, just a few weeks ago, we filed an enforcement action in California against a company called Nelson Gamble that was making robocalls, making this sort of debt reduction, credit card reduction type claims we’re talking about today. I know I spoke to consumers that began with consumer complaints. That’s how one of the things that led to that investigation where those complaints, even though the caller ID number was probably spoofed, even the location is probably spoofed.

That’s how we can help trace them back so we can look and see did someone pay money to someone. Did you pay $500 for the credit card debt relief? If you did, then we can trace that money back and we can find who you paid. Then if we bring an enforcement action and go in and shut down that company that you paid, then we can look through their documents and see who was doing the lead generation for them. Who was doing the robocalling for them? Who was the autodialer involved in the calls?

So we can go after everyone in the chain at that point, but it’s lengthy. It takes time to build these cases, to find the information, to trace the money back and then go in and actually get a court order to shut down the company to their records to just then end up finding out who actually made in the initial robocalls that was the lead generation that kind of sparked the whole thing.

We can also trace the calls back through the network. As they talked about this morning, that can be very difficult, talking about routing calls through all sorts of different carriers all around the country. It takes time to go back to each one and say okay, where did this call come into your network from? Now we have to go back to the next one. Where did this call come into your network from?

We can do it and it helps locate the bad guys, in many cases, but it’s a timely difficult process. We also use informants and former employees.

Not surprisingly, many of these bad guys don’t treat their employees that well. They don’t pay well. They don’t give vacations, and they end up with some miffed employees. We love to hear from them. We do all the time.

For instance, in that Nelson Gamble case, we used information that we obtained from former employees who weren’t happy with their former company, largely because they knew that bad that they were doing, and those former employees are an extremely valuable source of information when we trace back these calls and find the bad guys that are ultimately involved in these calls.

It takes time, but we can find them. What we do is we want to target those ones that are responsible for the most number of calls, the most bad. And when we do, we try to shut them down and get court orders to keep them from making those calls anymore.

We've got a lot of enforcement actions that I talked about already, a lot that have just been filed in the last few months, and there’s a lot more in the works and keep tuned to ftc.gov for more information as they come forward because I can assure you, more is coming.

MS. GREISMAN: Thank you, Will. General,

without giving away any state secrets, how do you find the bad guys?

MR. ZOELLER: Well, we've been very successful over the years. I've been told that it's past, I think, the wave of VoIP robocalls and cloud-based. So we're finding similar frustrations with spoof numbers and even where the numbers are valid, people aren't there. So we've gone through the same process we used to, but I will say that it's getting harder, with the new technology, to be as successful as we have been.

Some of the same things that Will talked about we're looking at. We are trying a couple of cases where the purchasers of the leads from lead generators are claiming that they did not cause the calls to be made, so we're going to be changing our statutes or proposing legislative changes that would allow us to get past that defense and require purchasers to verify that the leads were legally generated and not done through illegal robocalls.

We are also following up on another idea where similar to Will's suggestion that the boiler rooms don't treat people very well, we're going to initiate qui tam legislation that would allow anyone out there that might be working in a boiler room to call. If it’s really just about making money, they could probably make more money working with the Indiana Attorney General’s Office in a qui tam case than they could be paid by the robocaller.

We have been successful working with some of our state partners in being a little more creative where -- even there is one example, I think that was down in Florida, where we thought we had run into a dead end, but some of the people cleaning up after the boiler room saw all of the, say the scripts from the boiler room and called a few people. The next thing we knew, we had a live case.

So we are still being very aggressive. I’ll admit to more frustration with the ability to mask things and look forward to a little more help on the technological side to fight the new technologies that we’re battling.

MR. BASH: I don’t think I have a lot to add to what’s already been said. Obviously, there are challenges in identifying who these folks are. You would hope that you could use the number that is showing up on somebody’s caller ID to help you out in that regard, but I think we have heard over and over this morning, that’s often not a good source of information.

You can try to work backwards from taking, if not the originating number but the terminating number and trying to trace back to get the point of origin in that manner, but as you've also heard from a number of different people today, that can be challenging and time consuming.

Folks that we work with, carriers that we need to talk to often are very responsive and helpful in a relatively short period of time, such as, you know, a day or two, but that still can be a long process when you're talking about needing to get in touch with people, several different carriers who have been involved in the transmission of the call along the way.

Something like Henning talked about this morning that would be great is to get better intelligence about the true call, if you will, all along the way and to have a very expedited compulsory process vehicle available to get the information very quickly.

I also want to mention that I think it a challenge, if you will, that we have at the FCC that is not necessarily shared but the FTC and the Indiana Attorney General is you heard me talk about the fining process, which is the typical process that we use.

Obviously, there is law in many places, outlawing the type of behavior that we’ve been talking about this morning. But the worst actors out there don’t pay any attention to those laws. They may not pay any attention to a piece of paper from the FCC when we find them that says you’re breaking the law, we’re proposing a fine against you, here’s how much the fine is going to be.

So I think we need to be looking at the other enforcement tools that are available to us in the statutes, although they do not permit us, as I said, to go directly into federal court and seek an injunction. We do have sort of our own administrative injunctive authority that would have to be enforced in court. There is a Permission of Communications Act where the Department of Justice can get involved at our request to seek injunctions to stop violations of the law that we enforce.

Just to circle back to the penalty, something that I wanted to just follow up on, I think that Brad had mentioned earlier this morning. He was referring to penalties of $500 in the TCPA and $1500. Those are the penalties that are available for, I believe, private rights of action by individuals in the statute that the consumer himself or herself can bring an action to and join these types of practices or to get damages. States can do it as well, but the FCC’s fining authority is bigger than was mentioned. We actually can impose $16,000 per violation. So that means per call that is made, that’s a violation. We could impose a $16,000 fine. We, in fact, have done that in our most recent action.

The more common fine that we would impose is not quite that high. That’s the one that we would impose where there are a lot of aggravating factors involved. So I guess the point I’m trying to make is we’re using the authority that we have as aggressively as we have in terms of finding people, but I think we need to be retooling and looking at the other tools that we have in the Communications Act to address the problem as well.

MS. GREISMAN: Thank you.

MR. MAXSON: Along those lines as well, under the Telemarketing Sales Rule, we can go in and go into federal court and get orders to shut down businesses. As I mentioned though, sometimes that takes a while. So we are looking at ways to get into court faster so we can get into a judge almost immediately and say, we need to get an order to get these calls stopped and have these calls stopped going through the network.

Along those lines also, I can announce today that we’ve set up a honey pot with a significant number of phone numbers, numbers all over the country that come into our honey pot. The calls get answered and we record messages and take the information on the calls that are coming into our honey pot so that we can find out much faster who is actually making these calls and actually have the recordings in house so that we have evidence right there that will hopefully help us find these guys faster and file cases faster.

MS. GREISMAN: Thank you. I’m going to turn to some of the questions. There’s no shortage of them. There’s no way we can get through all of them in the remaining 15 or 20 minutes we have. We'll do the best we can. I’m going to liberally construe some and consolidate.

Let me start with the first one. Isn’t it better for the consumer to stay on the line, engage in conversation, collect as much information as possible rather than hang up? General?

MR. ZOELLER: No. You know, for years, we’ve told people that, and I think there may still be some benefit with a live caller. The robocallers -- we’re desperately trying to get the new word out that the longer that you stay on, the worse it is for you. So I do think that since the spike in our complaints are robocall based, we need to get that word across very quickly that it’s more a question of play the game of how quickly you can hang up.

MR. MAXSON: I think that’s right. If they give you information, it’s going to be fake information. The names they give you are going to be fake. You’re not going to get anything out of it. Usually, that’s not stuff we’re going to be able to use.

Also though if you press one or two, whether it’s one to talk to someone or two to be put on their Do Not Call list, because these calls are frequently coming from lead generators, they’re very happy to have you press either number because they’re not going to put you on their Do Not Call list. They’ve already broken the law by calling you with a sales-based robocall. They certainly don’t have their own internal Do Not Call List that they’re going to now honor.

What they do is then put you on more lead lists for people that are at home that have working phone numbers, that answer the phone, that listen to the message and press the number. So perversely, you’ll end up getting even more calls that way.

That may be different if it’s your school district calling you and legitimate, you know, your doctor or something like that. But for a sales-based robocall, we tell consumers it’s a mistake to press one or two, you should just hang up on them.

MR. BASH: I can tell you from -- I’ll admit to personal experience that it’s not particularly helpful. A number of years ago before I got involved in any of the robocall law enforcement that we’re talking about today, where I received a number of phone calls. I dutifully pressed one to say, no please don’t call me anymore. That did absolutely nothing, of course.

So then I decided to press two to talk to somebody about the product they were offering and that didn’t help. That made more calls come to me. In fact, when you start trying to get some information that might be useful to law enforcement, the phone gets clipped down. So people are not interested in talking to you about anything like that.

MS. GREISMAN: Next we have a series of questions on FCC, FTC coordination and also state enforcement under the TSR and TCPA. How’s it working? General, do you want to start us?

MR. ZOELLER: Sure. I think the states have banded together and again, the working group we go through the National Association has been very effective. I think our relationship with the federal partners has been, let’s say, as good as, maybe a little better than some federal agencies. At least, up until the last year and a half with the more technology.

We had a series of roundtable meetings around the State of Indiana to try to get some of our own issues in front of us so we could see what the state could be doing a little more creative use of our own state statutes and new authority, plus what things could be done at the federal level. Will was kind enough to come out for at least one of those.

I think in distinguishing -- you know there’re a lot of things about where these phones -- you know if you’re going to blast out 10,000 calls a minute, they have to be dropped onto the system somewhere. We look at it like, I’m not a big fan of regulation just for the point of regulation, but if you’re going to put 10,000 calls onto the system, it’s probably worse than radio. Can we regulate it, license it, put it into some way that the FCC might really focus on blasting out calls that will ring your phone at home?

I can always turn the TV or the radio off so

I don’t have to watch, you know, a dress malfunction or something, but I can’t turn the phone off unless I’m just going to cut off my communication with my friends and family.

So we are looking for more help and quite frankly in most of the conversations around the roundtables, they were looking to the federal government for more help, even if it comes at the point of more regulation, at least protect my Hoosier friends who just want to take a nap.

MS. GREISMAN: Will?

MR. MAXSON: Yeah, cooperation certainly is helpful. At least from my own personal experience in the investigations and litigations we’re involved in when the General mentioned the National Association of Attorney General working group that Indiana takes a bit part of and the FTC participates in. I know that that work group has been helpful, shared information.

There’s lots of states that have been helpful and are actually actively working with us on active investigations, especially when you have boots on the ground, you are aware our targets can be extremely helpful. It’s the same with respect to the FCC.

Obviously, you saw Henning here this morning, the FCC is here right now. We cooperate frequently with them. I personally speak to the FCC frequently. We share complaint information and make sure that we’re coordinating, not typically going after the same targets. So it’s helpful. The more states and more help we get from other federal agencies, certainly the better, but it has been very helpful personally.

MR. BASH: As Will said, the FTC and the FCC respective staff who work in this area do have regular and periodic contact to share information. If people are concerned about duplication of efforts, I’m not sure if that was part of the question, but you’ve heard that we have different kinds of enforcement authority. I think that’s something that would be taking into account in who might be the right entity to be pursuing a particular matter.

You’ve also heard that the rules, while there is a lot of overlap there, not necessary coextensive and without sharing confidential information that I of course can’t talk about specifically, I can assure you that there are state folks who are in touch with us about different problems that they are experiencing. We are working with them where we can and it’s appropriate to try to do what we can to deal with the problem.

MS. GREISMAN: Thank you. Will, this one is clearly for you. Under the TSR, does robocall including both autodialed and prerecorded calls?

MR. MAXSON: Yeah. Under the TSR, a robocall is a call that is going to be playing you a prerecorded message. So that’s what it is. By definition, it’s going to be autodialed. There isn’t going to be someone sitting there on the phone pressing in a number to play that prerecorded message to you. So absolutely, it’s the autodialed calls. What makes it a prerecorded call under our rule is the prerecorded message. The message has been recorded. It’s on the computer and plays for you when you pick up the phone. It’s not a live person you are talking to.

MS. GREISMAN: Thank you. We’ve had a lot of discussion about political calls and we did touch on it earlier, but there are a number of questions here, so it’s worth repeating some of the territory. What are the two federal agencies doing to enforce robocall to cell phone ban by political organizations?

And I think you probably first want to address the question itself.

MR. BASH: So obviously if you’re getting those kinds of calls that aren’t legal, file a complaint with us. We, as I mentioned, we’ve had complaints about that. We have active matters that we are looking into. Something you might be aware of to further get out the word and to remind people who want to comply with the law and who intend to comply with the law, what exactly the standards are.

We, from time to time, issue things that we call enforcement advisories that are really designed to highlight the agencies’ work in a particular area and even more importantly to highlight what the rules of the road are in a particular area and to alert people that we’re out here and available to receive their complaints. Just last month in September, given the political season that we’re in right now, we issued an advisory on what the rules of the road are for political calls.

So we are trying to get the word out. We do have complaints. We are looking at complaints and stay tuned.

MS. GREISMAN: Will?

MR. MAXSON: In the Telemarketing Sales Rule, FTC’s rule that crucial question basically boils down to whether a call is part of a campaign to try to sell you something. So if it’s a call from the Romney campaign or the Obama campaign, that wouldn’t fit within our definition because they are not trying to sell you something. Maybe they’re trying to get you to vote for them, but you’re not going to presumably pay them money for a service.

Survey calls, those types of calls, also fall in that same issue. They’re not trying to sell you something. Now, there are people that have gone out and tried to make sort of mask their sales calls as a political survey or something like that. Those calls are covered and we’re absolutely aware of those.

MR. ZOELLER: I’ll just throw in kind of unsolicited, our prohibition for political calls has been very successful over the 10 years that I’ve been involved in our office. Even though we’ve had a number of legal challenges and still go through it, it’s a pretty strong legal argument that particularly as it comes to blasting out tens of thousands of these calls to people who don’t want them in their home.

So the fact that we’ve got federal statutes on the cell phone, I still think that we’re going to be a winner on this idea that you cannot call people at home to try to get a political free speech, although that’s what the Seventh Circuit is still looking at.

Our argument is very strong that it’s regulating the time and place. It’s not going to be done over the phone in Indiana, unless the Seventh Circuit disagrees.

MS. GREISMAN: Thank you. Couple of questions on the same issue, what’s the magic number of complaints to trigger law enforcement?

MR. BASH: I don’t think there is a magic number. I think it's contextual in a lot ways.

MR. MAXSON: I would say the same thing. Most of our cases start out looking at complaints. We look at the complaints every day, all the time. They’re incredibly useful and we put everything into context. We look at what kind of evidence do we have? Do we have informants? Can we figure out where these people are? Are they in the United States? What are they doing? What kind of calls are they making? What’s the volume? Are they stealing money from people? All those sorts of things go into us figuring out who can we go after with our enforcement resources and stop the most number of calls.

MR. ZOELLER: At least in Indiana, you know, by the time you’ve hit the fifth complaint, it has already been triggered up the line. Again, you might have one complaint that really leads you to some very strong evidence. So, it doesn’t take much at the state level.

MS. GREISMAN: And, General, staying with you, there’s a question about criminal prosecution at the state level. Any success?

MR. ZOELLER: Well, I don’t know about criminal prosecution because our office has civil, so we would have to turn that over to local prosecutors or the U.S. Attorney. We haven’t been very good about, say, being draconian on fines.

We’ve had a number of very large fines. I think a lot of, let’s call it the legitimate telemarketing industry has a gold star next to Indiana essentially is not worth the cost of doing business. So whether you’re on the Do Not Call or not, at least up until VoIP, we’ve been very successful just using the civil penalties. If I catch Rachel, I will certainly look for a criminal statute.

MS. GREISMAN: Next question we have touching too many nerves. Do the federal rules supersede the state ones on autodialing?

MR. MAXSON: No.

MS. GREISMAN: Shall we move on?

MR. BASH: I will just say that I think there are some open questions that have been filed at the FCC on that topic and I don’t believe the Agency has addressed those questions, and I don’t think I should say anymore about that.

MR. ZOELLER: We would be inclined to have a hearing though.

MS. GREISMAN: One more question. Can somebody explain exactly what an autodialer is? Eric?

MR. BASH: I will tell you what the statute says it is. It is equipment that has the capacity to store or produce telephone numbers to be called using a random or sequential number generator. That is that statutory definition and also the definition in our rules of what an autodialer is. Hopefully that is helpful.

MS. GREISMAN: Well, we're going to actually end just five minutes early. There are a lot more questions here, but these are requests for legal opinions and staff opinion letters. I know there are a bunch of lawyers sitting out there and you all know there is a better vehicle than this format. I encourage you to take us up on it.

In any event, I appreciate your attention, and please let's give a round of applause for our participants. I also have a notice that somebody left a red Verizon LG phone. Please see somebody at the registration desk to claim it.

(Applause.)

(Whereupon at 12:20 p.m., a luncheon recess was taken.)

AFTERNOON SESSION

- - - - -

(1:25 p.m.)

CALLER ID SPOOFING AND AUTHENTICATION TECHNOLOGY

MS. GREISMAN: So we're going to shift gears a bit this afternoon. This morning we looked at the state of the industry, the state of the law, and today we're going to look at what's happening on the technological side. So we've got several panels that are going to take an in-depth look at what's available on the marketplace to date, what seems to be on the horizon, what's working well, what's not working so well or that could be tweaked a bit, and then we have an announcement later by David Vladeck.

So without further ado, I'm going to turn over this panel to Kati Daffan.

MS. DAFFAN: Hi. So our first panel of the afternoon is going to look at the problems of caller ID spoofing and call authentication and try to dig down a little bit into the technology and potential solutions in this arena.

We have an extremely distinguished panel here. I am going to just let you know who they are. They'll tell you how they fit into problem solving in this space. You've already heard from Henning

Schulzrinne from the FCC. We also have Adam Panagia, who is the director of AT&T's Network Fraud Investigations. Patrick Cox is the CEO of a company called TrustID, and Vijay Balasubramaniyan is the CEO and co-founder of Pindrop Security.

So without further ado, I will turn it over to Henning.

MR. SCHULZRINNE: Good afternoon. I want to start out by describing a few possibilities that might emerge as we transition to all the requirements so that we can better secure an infrastructure that we all rely on.

Our focus here is clearly on robocalls. I do want to point out that there are many other problems that occur due to particular spoofing on caller IDs. Individual fraud, phishing attacks where individuals are targeted, not by robocalls, but by criminals who want to obtain items of value, whether it be their password or be it banking transactions are also enabled by the same fraudsters.

First of all, caller ID spoofing itself is illegal if it is used for purposes of intending to defraud, cause harm, or wrongfully obtain anything of value. It is not illegal, as there are applications of caller ID spoofing that are seen as at least harmless or, in some cases, desirable.

The classical example of that is a doctor using his or her mobile phone, who obviously does not want to reveal that phone number to the patient he or she might be calling and wants any return call to be returned to the doctor's office, not to their personal cell phone.

In that case, the person is a legitimate user of that number, but is not using a device that is assigned that phone number. There are various women's shelters and so on, where one can make a case that this serves a legitimate purpose but in a very restricted fashion.

So generally speaking, in our case, certainly caller ID spoofing would generally be considered against the Caller ID Act of 2009 because it's generally used with the intent to defraud or cause harm or other damage. Let’s look at what we can do. There are really two techniques at the numbering level that I think deserve closer scrutiny.

The other techniques that some of my co-panelists I believe will talk about, which take a larger view of the overall ecosystem as to how we can identify possible malicious calls, robocalls, in general, that don’t necessarily rely on the numbering information. But numbering information, as I pointed out in the earlier presentation, is crucial if we want to have black lists and white lists, both for an individual basis as well as on a larger scale basis.

The first mechanism is the authentication of the number itself, currently because if a system, as Steve Bellovin pointed out in the morning, was designed, if you like, in the pre-cryptography era. They were trusted entities and for a variety of technical reasons, it really wasn't feasible to process enough data to assign calls. All of this meant that there's surprising little cryptographic information, if any at all, in the traditional landline system. It's a little different in the cellular system.

Number authentication, the way it would work is that if you have a call record coming in -- and I'm showing it here on the slide an example of a pretty good approximation of what a VoIP would look like. It looks kind of like email, but it contains, essentially, information with either your telephone number or a user name and date and other information related to that.

Since about 2004, we've had technology available that allows us to sign these records, whether it’s public/private key pair, similar to what we would use through email, or more familiarly, a webpage. We can use that technology, again, it's not widely deployed at the moment, but it is not a standard challenge, it is a deployment challenge.

If we look at caller identification, we really have two kinds of cases. I think it’s helpful to look at those separately.

The first point is that we have known callers, your grandma calling. I have talked to them before. I know their phone number. They're in my address book. I've had previous contact with them because they have sent me email with their phone number attached and so on. I can recognize those.

We have to do a better job of automating recognizing the good callers so that we have a lesser challenge of identifying the bad ones. But we also have a number of legitimate calls where we wouldn't necessarily recognize the caller ID, even if it is certified in some way.

What we do care about in that case is not so much what is the phone number that is coming from what purports to be the credit card agency, but is it really Visa or MasterCard or the bank that I have, as opposed to somebody who is trying to do me harm.

I don't care about the name of a person who is calling. That doesn’t really matter to me. It's just another staff person. What matters is, is it a bank or is it the Social Security Administration or whoever it happens to be. That, I think, is a problem that we also need to solve, namely, identifying securely the entity that we have.

We've been looking at opportunities to look at what’s known as attribute validation; namely, validating the attributes of callers that we couldn't do before in the traditional telephone number, but now we can.

Where, for example, an entity would contact -- and this goes back, again, to one of the panels in the morning -- a legitimate mass caller, now our theme, would be able to obtain a credential of a trusted entity, such as a government agency, a school district, something that I would recognize as a recipient of a call.

They would be able to convey that information and say, yeah, I believe I'm entitled to that. And if you don’t believe me, because you have never met me, go contact this trusted entity, a webpage of, say, a school district, and they will vouch for me and say, yes, I'm acting truly on their behalf, as opposed to I'm just pretending to be a school district or pretending to be the Social Security Administration.

And then I can use standard web-based authentication techniques to validate that this is indeed an entity that is allowed to speak for that particular call.

So there is a mechanism, again, where the call itself just simply contains a vouching piece of information which is invalidated to somebody else. We are currently exploring that technology. It is not a standard yet, but it illustrates the kind of techniques that we might be able to use to go beyond just simply validating numbers.

In general, we have an opportunity, now that we have cryptographic capabilities, in end systems -- no more dumb phones -- that can validate certificates just like your web browser can. We have an all IP path increasingly that can carry additional information and a much more extensive system than we had before in the old days, a seven system. With those two facets, there's really no excuse not to have a validated, traceable origin authentication phone calls.

With that, I hand it over to Adam.

MR. PANAGIA: Good afternoon. First off, I want to thank the FTC for inviting me to speak on this panel. This is a serious and growing issue for the industry. I believe that the people in this room and the people listening to the broadcast really need to get together, whether it be law enforcement, regulators, carriers, technology companies to kind of join forces to figure out how we need to solve malicious spoofing and malicious autodialer or robocalling issues.

My name is Adam Panagia and I'm the director with AT&T's Network Fraud Investigation Team. My team is responsible for prevention, detection and deterrents of fraudulent schemes that are perpetrated against AT&T and its customers.

Let me give you a little background on how we get involved and how I got the thankless job of looking at robocalling investigations. We deal with traditional toll fraud issues. We deal with identity theft issues, subscription fraud where customers sign up for service on our network with no intention of paying for the bill. We deal with account takeover issues. And then I have a separate team that deals with intercarrier compensation fraud. This is where telephone companies are sending traffic back and forth and trying to do something with the record. So they either inflate the expense that another carrier would owe or they bypass revenue or expense obligations.

Given the fact that we have these tools in place and the systems that we use, we process about four billion call records per day. So some carriers are looking for a needle in a haystack. We're looking for needles in stacks of needles.

Huge amounts of volume of data that we're looking through continuously. So since we have some of those skill sets to look at traditional fraud type operations, about five to seven years ago we were tapped to start looking at robocall-type activities and malicious spoofing activities as well.

I'm going to pass a couple of these because they were covered earlier. I just want to really focus on this definition because customers, people who come to me and say, Adam, why don't you just identify the spoofing activity and why don’t you just block it? You know, you're the phone company. You can do that. There's technology out there.

Well, you know, it’s very, very difficult for us to identify a spoofed call, especially real time. Now, after the fact, we have techniques that can go and positively identify whether a call has been spoofed or not. But as the call is traversing the network and transiting the network, we don't really have a way to identify that. Now, some of my colleagues on the panel will probably speak to some solutions they may have in certain areas.

The other thing is that there is a challenge to identify it. Now you're talking about blocking it. There are crazy things being thrown around like let's have this spoofed number list that everybody has and everybody blocks. Well, I can’t tell you how many times I get customers -- they may be large financial institutions; they may be government institutions -- that come to me and say Adam, my number is being spoofed. You've got to do something. You got to block this. And we say okay; we have to research it first because we don't just block, we thoroughly investigate everything.

So as we're looking through this, we find out that that bank actually contracted with a third party and gave them permission to spoof out their number on some telemarketing campaign. But the person at the bank that was talking to me didn’t know that. So the left hand didn't know what the right hand was doing there.

One of the things that we'd like to do is really thoroughly investigate the spoofing activity before we take any action. I'll get into some of the actions that we can take in a moment. The other thing is there have been a lot of discussions surrounding some of the spoofing capabilities that are out there, some of the legitimate reasons that you're going to spoof and some of the more malicious reasons.

Well, another interesting kind of play here is AT&T may contract with a third party to perform customer service and we'll give them permission. We like to say spoofing with permission. That's what we're calling legitimate spoofing versus spoofing maliciously, where nobody has permission to actually send those calls or deliver that hand for the network.

Now I'm going to move into the more malicious spoofing. This is the definition here, the practice of sending false or misleading information so as to deceive the receiving party and hide the caller's true identity or call origination. So this is what the malicious robocallers are doing. They are not only spoofing random numbers, they're spoofing numbers of our customers. I'll get into a little bit of what that does.

They're not only spoofing 10-digit numbers, they're spoofing 16-digit numbers. They're spoofing three-digit numbers. I've seen calls come across as 007 as the originating number. So they have these super computers that are tied to VoIP networks that are programmable. They can do whatever they want.

I'm going to kind of dive in here a little bit and just try to give you a high level of understanding of what a robocall flow looks like. I'm going to dive a little bit deeper, again, into the trenches a bit on how these calls traverse the network; how they multiple-carrier hop, and how there are multiple protocols.

Before I get to that, when you look at this black box that says, "Mass calling generator and spoofing capabilities," what we're seeing on the network, what’s coming to my team to investigate are call bursts of, within four hours, we're looking at 10, 20, 30 million calls going out across the network within hours. It’s not targeting particular states. They're marching through MPA and XXs or area codes and exchanges.

So you have over here in D.C., 202-456-0000, 10999. That's a 10,000 block of numbers. We watch them march through every single number. They don’t know, necessarily, who they're targeting. They're targeting wireless customers, traditional landline customers, VoIP customers and multiple different carriers that own those numbers.

So what we're really seeing is an egregious attempt to either deny somebody service with these robocalls. We're seeing that they're trying to sell some underground or worthless product, as was discussed before.

Let me just go through this call flow very quickly. The mass calling company, the black box and the robocaller box is really one in the same. That's just really the traffic pump, if you will. As the robocaller gets service, and as I explained earlier, the service is very cheap, easy, fast to get.

The robocaller will typically have an arrangement with one provider. In this example, the robocaller has an arrangement with Provider A. So this robocaller can be anywhere in the world. Basically, Provider A said send all your traffic to this IP address and let it go. So the robocaller starts generating this traffic and it goes out to Provider A. That connection is Voice over Internet, what Henning was discussing before.

Provider A may have a PSTN connection, a Public Switch Telephone Network connection, to Provider B. So now Provider A converted that from a SIP or a VoIP protocol into a traditional circuit connection and went over to Provider B.

Provider B may then convert that call back to VoIP again to C. C converts it back to the circuit base and then it gets over the interconnect arrangement to AT&T. So now we're getting this call when we deliver the so-called last mile to our business or consumer or wireless customer there. So now we're going to work this backwards.

So now you've got a customer, or multiple customers, or hundreds of thousands of customers that have this strange caller ID that they don’t recognize. They've got some kind of automated announcement and then the complaints start coming in to all of the agencies. Now law enforcement or the FTC or the FCC need to get involved. So what can they do?

AT&T, in this particular instance, can only see that the traffic came from Provider C. Folks think that we can see all the way back to the robocaller and that's just not the case. When a legal demand is submitted to AT&T, we'll say yeah, it came from Provider C because we know that. We have the interconnect. We don’t care if the number is spoofed because we know that it came from Provider C; we know their name. Now, that happened to be a circuit connection.

Law enforcement has to go to Provider C. They may say to law enforcement, okay; great. I'm not too sure about the number, but my records show that this came from IP address 123xyz. So now law enforcement has got to go, oh, God, now I got to go chase an IP address. So they chase the IP address. And if they're lucky enough, they're going to get back to Provider A, who was another circuit-based connection. So I'm just trying to highlight the manual difficulty of tracing these calls all the way back.

Now, it's been done. It needs to be done faster. Having spoken about the Truth in Caller ID Act, if we can find that these guys are defrauding and getting something of value in using spoofing technology and we can trace it back faster, I think that's one of the ways we can get some of the bad guys off the street in these particular instances.

Last slide; this is kind of how my team sits in the network. When we get that heads up that there's a spoofing event or there's a mass-calling event, we typically get them from our wireless knot. We get them from our global network operation center. We do take complaints if there's enough of them aggregated. But this is where we're sitting. My team is sitting in this little box called local service provider. And that's just one of our networks, right.

As far as the local service provider, now, the mass caller sends these 10 million calls out. He's linked up with one VoIP provider. Well, that VoIP provider can’t handle 10 million calls, so they have redundant routes. They have overflow routes. So the VoIP provider sends it to Provider 1, 2, 3, and they send it to G, E, B, and A. So they're sending it to four or five different carriers. Then those carriers are sending to other carriers.

(Brief technical difficulty with facility audio system.)

MR. PANAGIA: So as we're sitting in that box, that local service provider box, we are watching traffic come in from seven different carriers. Now, that's our local service. All right. We're the incumbent provider in 22 states. We're the dominant provider. We also have a national CLEC network. So we have these switches and service across these networks. We also have a huge wireless network with a hundred million plus customers. We also have a vast international network.

So take that box and multiply it by five and then multiply it by however many carriers are coming in, I'm seeing this traffic come in from 24 or 25 different carriers. What we try to do to help our customers and help our network is we measure the traffic. We try to find the carriers that are delivering the most traffic across our network, in total, and reach out to those carriers and ask them to cease and desist any illegal spoofing or robocalling activity.

So that’s kind of what it looks like when we're -- you know, this is very basic diagram. It's kind of what it looks like in our world. I'll just mention one other thing because I think I'm running out of time here. You know, protecting our customers, protecting our network is really at the forefront of what we do.

Many times, that black box is sending out one of our customer's numbers. So if our customer's number goes out to tens of thousands or millions of telephone numbers, these people start getting curious and they call the numbers back.

What does that do to our customer? It actually deploys what we call a telepathy denial of service attack on our customers. So everybody out there that gets these phone calls and you're calling a number back, you may be calling an innocent customer that the bad guy used to spoof its number on the caller ID, and those we take very serious because we have customers that have had their phone numbers for a year, 20 years, 30 years, 70 years. Now they can’t use their phone because every time they pick it up, a new phone call is coming in from a curious person that received an autodialing with their caller ID.

That's just one example of what we're seeing, but I'm going to move on to the next panelist.

MR. COX: I'm Pat Cox. I'm the CEO of a company called TrustID. We're based out of Portland, Oregon. I'm happy to be here today. Thanks, Kati, for having us out here. I'll kind of start with the end in mind. I don't have a solution that deploys easily at a consumer level, but the great news is that we're coming through with some really high quality solutions at an enterprise level. We can really determine when a call is valid and when a call is invalid for large-scale business users. So it's a step in the right direction.

What we focus on is what is helping companies today, serve their customers and not serve our criminals’ needs. Pretty simple concept. Really, the way we do that -- I think it's been addressed to a great extent today -- the problem with the way we do that is by analyzing the originating source of the call in real time, before the call is answered, to determine whether the call is coming into a bank or a large call center, a utility company, or whatever it may be, is real or is not real.

Obviously, up to about 2004, this wasn’t such a major concern. The internet had not yet connected in a very deep and meaningful way with the telephone system. When that happened, however, almost every thread that we're aware of on the internet is now making its way over into the telephone network, which is a really very different landscape than the traditional telecommunications enterprise, large-scale business and us, as consumers, with phones themselves, are used to. We're used to being able to trust the information that came in, back when the telephone numbers were a closed, trusted, certified network. Not the case any longer.

How do we do what we do? This slide is a little odd, but hopefully we can get it there. Step 1: A call comes into, let’s say, a financial institution, a call center. The carrier doesn’t change, so if Adam is routing a call from the client into the bank, that stays the same.

Step 2 for us here is that the call center, because they've got a large PBX system and they've got specialized trunking that they probably get access to information called ANI, A-N-I, which is a bit different than caller ID, caller ID is a little easier to spoof. Not a lot. ANI is pretty easy to spoof, too, but a little tougher. ANI will come on most callers, whereas caller ID can be blocked.

As citizens, we have the right to say we don't want to transmit our phone numbers. We block it for privacy reasons. But ANI, when you're calling an 800 number and the bank receives the call, for example, the bank is paying for it, right. They're paying for the toll. So they have some right to see who they're paying the toll for. It's like someone knocks on your door and you have the right to see who's there before you let them in.

That's how the ANI information comes in. We get that ANI information sent over to us as soon as that call hits their number. So it's even before the call is answered. What we then do is look at the network -- as a carrier, the network ourselves -- and determine the validity of the call. Is the call real? Is it the claimed ANI -- we call it a claim, right, because it used to be an identification factor, but now it's just a claim.

Is the claimed ANI real? Is that cell phone, is that landline phone, is that Voice over IP device, or is that payphone, or whatever it might be calling?

In many cases, of course, we'll see that the numbers are pager number. Well, pagers can’t place outbound calls for the most part. It's a good hint that something's wrong. But we delve much deeper than that into the network, make a determination, in real time, as to whether the call is good or bad. Simple measure, green or red we call it.

Once we have that answer, we send that information back, that trust metric, if you will, back to the call center or the bank or the large institution with the big PBX and these fancy PRI lines, and so on, that give them that ANI information that we need to have to do our work and let them know.

They can then take that one step further and say well, now we know it's a real call. It's a green call. Does that number match the number on file? Do we have a fraud flag? Is it on a watch list? All sort of analytics can come into play to help authenticate that caller. So it's a powerful solution for caller authentication, but the other side of the puzzle, really, is not just the green.

The good news is no matter how big the problem is that the super majority of the calls that are being made are still good, most of its good. But that small slice, that small segment, the red slice we call it, isn't always bad. I think Adam made that point. In many cases it's the bank delegating some survey, or whatever it might be, to a third party and they send the number off because they really are representing that bank.

The number has been changed. We can tell that. We'll say this isn’t coming from the claimed source. So it would be red, but it doesn’t mean it’s always bad. It doesn’t mean it’s always malicious, which makes for the challenge we have.

At that point, if you start blocking the transactions, blocking the calls, we might be blocking a highly important emergency alert call. It might be blocking a call from your son in Iraq. It's problematic because the numbers change and the network sometimes do things when you roam within cellular towers because we're looking at the ANI. We're looking at that ANI, the billing number. A lot of it has to do with money. So numbers are changed to make sure the right parties get paid, but we can tell them if it is green or red.

So it's highly powerful for being able to say this 95 percent of your call flow, bank, is trustworthy and you know it's good. Now, the good news is that the red segment becomes the needle in the haystack, versus the needle in the needles.

So not every slice of red will be bad, but now we can shrink that pull-down and say okay, look in this segment of calls, that’s where the criminals will be. I mean, no criminal in their right mind robs a bank without a mask or a baseball hat or a pair of sunglasses or something.

So why would you rip off a bank or some other institution by calling from your true home number? It just wouldn’t happen. The police would be there in a few minutes and it's over with.

So this is where the fraud is. This is where the criminals are. But just because it's red, doesn’t mean it's bad, but that's where it would be. That's really what our technology can deliver to enterprises. We really don’t have a fantastic way today of transitioning that into a consumer environment, but obviously we continue to look at ways to do it. Obviously it would be a powerful tool if you could. That's what we have today.

So I'll pass it over to Vijay.

MR. BALASUBRAMANIYAN: Hi. I'm Vijay Balasubramaniyan, the CEO and co-founder at Pindrop Security. A little bit of background before I get into my presentation. Before coming to the U.S., I did my undergrad in India and worked for a long time at Siemens, where I wrote telecom-switching software. So I know the old style telecom system really well.

I also worked at Google, where I wrote the scale algorithms for the Google video chat products. So I know the new age Voice over IP kind of systems well, too. I came here to do my Ph.D. I got my Ph.D. from Georgia Tech in the Information Security Center. So I'm very well aware of web security, email security, and my focus area was telecommunication security. We founded Pindrop Security based on Ph.D. research that I had done.

With that in mind, before I start off, I mean, you've heard a lot of our caller ID spoofing. This is information from our phone fraud report, where we are constantly monitoring what the kind of fraud activity a lot of these bad actors are doing. And we're able to have that kind of visibility, largely because of our customer base. The fact that we are actively monitoring the email, the web, and our own honey-potting infrastructure to identify we know fraudsters.

We, right now, have the world's largest database of these fraudsters. So what we're able to do is we're able to identify what kind of activity they're up to. And as you can see, one of the biggest things is that the activity is constantly increasing, right.

This year alone, the activity has increased by about 30 percent. Also, you know, most recently -- well, yesterday we dropped the report for tutoring this year and it shows the same print. It's going up. It's going up by 30 percent. The reason I put in facts is because I love facts. Data is never wrong, it always tells you where to go.

The other thing is our technology allows us, just by listening to the audio, identify what type of device was being used on that call. So we have fingerprinted a lot of these fraudsters. Identified what kind of devices they're using, and the large majority of them use Voice over IP. There's about a 40 -- I think it's 46 percent of Voice over IP systems that are being used by these fraudsters.

The reason that they're using Voice over IP -- I mean, we've talked about it a lot -- is Voice over IP allows you to be anonymous, allows you to make it largely automatic, and it's extremely inexpensive. So these are the reasons that they are always gravitating towards Voice over IP.

In addition, there are service providers who actually allow you to pick a number every time. So for example, if you are targeting people in Washington, D.C., you can actually pick a 202 area code and say I'm calling from your local branch. You know, I really need you to give me this information, otherwise I'm going to shut your account down. And that's a very powerful way for a fraudster to attack you. And we've seen a lot of this.

Finally, it doesn’t matter if you're in a high-density population or a low-density population. These fraudsters are going after people everywhere. Because of all the data that we have, we have some very interesting analysis.

For example, until the beginning of this year we found a lot of fraudsters were using phone numbers from a really remote part in New Hampshire. That part has a population of 253 people, but when they were assigned number blocks they were given 10,000 numbers. So there are not enough people for numbers. So it's very easy to obtain those numbers in bulk.

Right now it's actually moved all the way to the west coast. There is this county called Tillamook County, which is up in Oregon where Pat is from. They are known for they are known for their trees and their cheese. Nothing else. There are not many people, but a lot of fraudsters are picking numbers from there. So all this data allows us to really understand what they're doing.

So now comes what we do. So the funny thing is because it's Voice over IP, there's an app for caller ID spoofing, too. You can use their app and you can pretend to be anyone. Anti-spoofing is not harder, especially considering what Adam said, the network actually travels through so many networks in between. It's very hard to find out what the source is. It's extremely hard to identify.

Fraudsters have been around for a very, very long time. They've used these techniques in the internet world really, really well. Now you've just said I'm going to open up the phone network for the internet world. So they don't have to change their tactics, they just figure out how to make it work.

So what does Pindrop do? Pindrop, right now, we are an enterprise. We provide solutions for enterprises. You know, we have financial institutions as customers. So right now financial institutions use just knowledge-based authentication questions.

The reason it’s important to understand, you know, we're talking about consumers, but the fact is that a lot of these fraudsters are getting your important identity information to essentially go withdraw it from your bank account or withdraw it from some other place.

So what ends up happening is if you see the money flow, it’s always one of the places where it’s financially motivated. So a lot of these enterprises, what they do is they use knowledge-based authentication questions. What’s your Social Security number? What's your mother's maiden name and all that.

It's funny because these questions are extremely ineffective. For example, we've seen this case where this person actually started off with one name and changed his name midway through the phone call and still managed to get through the call center's agent. Largely because the call center or the agent's job is to provide customer satisfaction, right. And they're not here to stop fraud. So knowledge-based authentication questions is really not very effective way to do things.

So what do we do? Because of massive data analysis, we are able to identify well-known fraudsters as well as the fingerprints that they come from. So if it is -- what we do is we have acoustic fingerprinting technology. This is technology that we developed, as part of my Ph.D. research, where this acoustic fingerprint is able to identify any phone device in the world. So we are able to just listen to the audio and be able to assign a fingerprint. This fingerprint allows us to not only identify that phone device, which is how we're able to identify known fraudsters if we've ever seen them.

We are also able to use anomaly detection to identify brand new fraudsters. And the two big things that we do is just by listening to the audio of the call, we're able to identify what type of phone device was being used. Was it a landline? Was it a cell phone or was it a Skype phone or the Magic Jack phone? Or a lot of these fraudsters use this device called Two-Way Talk. So it's in that kind of form.

The second thing that we're able to do is we're able to identify coast range geography for the calls. So we can listen to the audio of the call and tell you the geography is the size of France. For example, we can say this is a call coming from the east coast of the U.S. or the west coast of the U.S. Or it's not at all coming from the U.S., it's actually coming from Nigeria or Eastern Europe.

So you then start seeing what you can do with this kind of technology. So you are getting a call from your pastor. He's not going to be calling from Nigeria on a Skype phone, right. It's highly likely he's calling from down the street. So this anomaly detection, the fact that the incoming signal, the audio signal, is very, very different than what it's supposed to be, allows you to identify a whole lot of things.

So anti-spoofing detection is one thing that we do, but it's anti-spoofing detection with intelligence. It's not just saying is this ANI being spoofed. ANI can be spoofed for a variety of good reasons. But is this ANI being spoofed and are you getting a call from China, when that's not what you're planning or that’s not what you're getting or that’s not what the profile of your customer is.

So with these new technologies, this is how an acoustic fingerprint looks. What we do is we use all these views, you know, we use 147 different features. So it's very similar to companies on the online world, like 41st Parameter and things like that, which look at your IP address, your browser settings, what service provider you came from. All of that to essentially identify the phone device -- identify the computer that's logging on. So that allows them to say yeah, this is a Lotus transaction. We do actually that on the phone, but at a far more granular level.

So we use 147 different features, including things like line noise, artifacts left behind by codec and all of that to create a detailed profile for the form. And we can say, you know, this particular device that we've seen before, so it's your legitimate customer. Or this is a well known fraudster that we just saw targeting Bank of America and we know from their form fingerprint. And we'll know if the type is mismatched or the geography is mismatched and then we can provide a risk code for every single call.

So what happens is that as soon as a call comes into bank, our analysis kicks in and identifies whether this is a legitimate or not and then what it does is it then says, you know, this call is this risky. So it's highly likely that that's a fraudulent call, and then the bank can take action.

The same way, that's what we want to do with consumers, too. We will provide all this information. And once we provide all this information, it's up to the consumer to make that decision. We believe consumers, once they're empowered with the right information, or a bank when it's empowered with the right information, can make that decision, even on those boundary cases. And then they can tell us, you know, you were right there. You were wrong there. And that's the only way you can learn.

Protecting the ecosystem, what we believe, you know, the grander vision for any system that is protecting the ecosystem we think should protect, one, enterprises. You would not want your bank account to be drained out. One fine Sunday morning you don’t want to wake up and see that your bank balance is zero dollars.

The second thing that you want to do is protect the carriers, right. Be able to provide some kind of empowering information to these carriers so that they can decide what to do. And finally, protect individual consumers. Being able to tell the consumer that this is a call which is coming from your friend or if it's coming from a very, very different location. Or this is a call that's coming from America, but it's not coming from Bank of America at all, it's actually coming from some Skype phone in Nigeria.

So all this analysis is part of Pindrop's core technology. Thank you.

MS. DAFFAN: I'm glad we have significant time for questions for this panel. I wanted to start off by talking about if we're looking forward to how can we help combat malicious caller ID spoofing. I would like to take a moment to say what can government agencies do? What can Congress do, if anything? What can industry do?

So if we could just take each of those in turn and talk about those.

MR. SCHULZRINNE: I believe your question implicitly hinted on that it's not a single entity that can do that by themselves; it has to be cooperation among all of those.

In particular, I would say this has to be one where it’s a combination of making technology available, encouraging its widespread use because as was pointed out in one of the morning presentations, one of the problems is we can probably identify the good calls relatively easily of those that are willing and able and have a interest in identifying themselves, but that will leave a large number of calls that have no identification.

Since many of those will still be good calls, non-robocalls or non-fraudulent calls, that makes the overall system much less valuable compared to when almost every call that is legitimate is indeed identified.

On the last side is where the regulatory side, policy side comes into play to where we can encourage widespread adoption, shall we say. I do see opportunities. We're looking at the Commission and numbering in detail in particular, as to how numbers are assigned. Who gets numbers, what does it take to get numbers? And that offers an opportunity if you have a valuable resource of numbers, people want numbers because they allow them to interconnect to a global communication system to be reachable. Well, that's also responsibility.

Responsibility means you have to be able to be identifiable, as appropriate, or at least you have to know that this number is not the one that you've been assigned to for a variety of reasons. We need to be able to deal with the issue of numbers that are used legitimately by non-circuit owners. So I believe particularly in this world where we're looking at new number assignment mechanisms.

At the Federal Communications Commission, we have an opportunity to provide much stronger identity requirements and identification requirements and then we need industry to play along to actually implement standards, to carry data end-to-end. We have a big problem that data gets lost along the way. I mentioned test room border controller, and Voice over IP has this tendency to strip call-tracing data from a call. I believe that is extremely detrimental to our ability to deal with fraud. It's often done for competitive reasons, but it makes life much more difficult and we may need to come to an agreement as to what is stronger, and we should have more weight, in way of protection, against fraud and abuse, relatively for pure commercial interest.

MR. PANAGIA: I envision an ultra-modern Batcave boardroom where I have an FBI agent on my left and I have a prosecutor on my right, and I have all my carrier colleagues in the room and we can ring the bell when the autodialing event happens. So kind of on a serious note, I think we all really, within the lay of the law, we all really need to be working this together. The FBI agents don't know what we know.

The FBI agents don't know what we know. The telephone company investigators can't do what a prosecutor can do. So we really need to pool these resources together and really figure out a way to trace this stuff upstream as fast as we can and get to the bad guys. Put fines on them. Put them in jail. All the things that these panels talk about. That's kind of my wish.

MR. COX: Being sort of in private enterprise, I look for solutions that can be implemented today. That's the world I live in. And the future in great, but in the future I'll be dead. Things happen, right. So the way I have to look at is I think the tool today is what you guys are doing right now, education.

I think businesses quickly understood that information coming on the phone network may not be completely predictive of who is on the other side of that transaction. I think the worker who is going to educate the consumers of that as well is important because, frankly, at the end of the day, we have privacy rights. And we can just choose not to transmit a caller ID blocked caller. Well, the spoofers can do that as well. So you pick it up and you don't have what you have, right?

That caller ID information that you get and we kind of rely on, the relying parties is broken. I think just having people understand that. I bet all of you understand that clearly, but I bet if you polled most consumers today you'd find a limited amount that would really understand that that number is not completely trustworthy. And if we can educate and get people informed that hey, it's useful, but you can’t rely on it. Don't give out your bank account information just because it says the call came from Citibank. All right. That is something today that can reduce the fraud, reduce the damage. We were talking about apps. It absolutely makes total sense.

I've been in telecom all my life like you guys and I've always wished -- we've got these great standards. You look at what SS7 could do, but it’s never complied with. Standards are tough for telecom because it's a global network. It's not within the purview of the United States. It's globally connected. It’s the second largest network in the world. So trying to enforce standards that are going to be followed every time is tough. As long as you got one person violating it, then that's the hole, right. So I think education and raising awareness. The website that you guys are putting up is very powerful for today.

MR. BALASUBRAMANIYAN: If you want to see how this thing is going to play out, we don't have to look very far. In the early 2000s you had spam, which was a huge problem. The government introduced the Can Spam Act and that invalidated a lot of people from sending out spam information, and then technology kicked in. Lots of people use IP blacklisting, content filtering, all of that to build an ecosystem that pretty much now makes email a sort of usable tool.

I say start off because I always think there's room for improvement. But that's exactly the way the security in the phone channel is also going to go. The fact that everyone is now realizing that there is a significant problem, means everyone is going to band together to come forward with solutions. The government and regulation is going to put together an act. And the technology industry is going to try and come together with solutions.

Adam mentioned earlier, trying to identify where this call is coming from. The question is AT&T, since they have been working on this for a very, very long time, they have really sophisticated tools that allow them to identify.

If someone tells you, you know, you got this call at 12:00 p.m. today, you have to go through all your call records and find out who that service provider is and make that connection and then do it for a variety of things. Look at different views to try and identify, okay, who do you go to next. It's not that a lot of these telcos don’t want to do it. They just can't. They don't have that kind data-mining infrastructure.

So another technology company will come along and help them do that. So as these technology companies grow and grow, you will start seeing the problem getting solved. I mean, it's the standard human model. All of us is the human network. We will all get together to try to solve a problem if it causes enough pain. That's how I think it would work.

MS. DAFFAN: A question for Vijay about Pindrop

Security. How do you determine the origin of a call or the location, based on the quality of the line?

MR. BALASUBRAMANIYAN: So the way we did it -- without giving away too much -- an example is -- I mean, there's a very simple example, and that’s one of our features. For example, in the U.S., on the PSTN lines you use a particular codec and it's called G.711 u-Law. Anywhere else in the world you use a different codec. You have what is known as G.711 a-Law.

Now, that characteristic, just the fact that something is trying to capture your voice, it captures your voice very, very differently. The analogy that I would like to use is if you're playing the same song on a Fender Telecaster or a no-name guitar, it would sound very, very different because not only is it a question of who you are and how you're playing it, but it's also about the instrument.

If you're playing on a really crappy instrument, if you're playing the best song, it is going to sound bad, and that's exactly what happens with these geographies.

Different countries have different infrastructure lists. And that tends to add very, very specific artifacts into the audio of the call. The audio is something that is very, very nice. It’s one of those things that is very valuable.

It's like if you were traveling through a bunch of places, collecting the sediments from all those places. The audio does exactly that. It collects artifacts from every place that it has visited, and when it finally reaches your shore, you can actually look it and say, oh, it's been here, it’s been there and then it's come here. You can't obviously do it in an extremely fine grain level, but you can do it at a coarse grain level, good enough to make some interesting observations.

MS. DAFFAN: We have two related questions here. Both people noted that the technology solutions we've been hearing about are enterprise-facing. One person said is that because consumers are not willing to pay or the solutions will just not work in a consumer setting?

Another person asked would carrier and service providers have to do more, including cooperate with each other, in order to come up with solutions that face end-users?

MR. SCHULZRINNE: Let me just take a stab at that. The reason, in both of those cases, it's really a vendor solution is because in one case it's information that's only available for the other numbers, which most consumers don't have. And the second one is that the audio identification, obviously, that's not a Rachel problem. I don’t need an app to do that. You’d have to receive the audio beforehand. So it helps with the important problem and fraud is probably less relevant for the robocall type of events because a nuisance happens as the phone rings, not so much the call itself.

I do believe there is a need for closer cooperation, simply to allow third parties more access to the call flow, my trusted third parties. So one of the things that happens in email in some cases is that you could add a third party to your email chain relatively easily so that if you decided that you liked that particular company or an open source product to identify spam, you could do that without changing your complete email system around. We don't really have that in the telephone system.

We don't have the ability, for most consumers, to hook in on third-party services that allow identification. That's becoming possible. There are now APIs that are being published by some providers. So having more of those, as we get more trustable information, will then allow third parties, on behalf of a consumer, to do that, but that’s just not feasible at the moment, given the architecture that we do have. We're starting to change our smartphones because that's why we have the ability to intercept calls before they ring. It’s a little harder on a landline phone today.

MR. PANAGIA: As far as protecting consumers, we have products. And when I say "we," the telecommunications industry have products that could -- anonymous call rejection, anti-block list, that kind of thing. But everything that’s been developed up to this point has really been telephone number or ANI-based. As we learn, through this summit, because they can dynamically change the telephone number so quickly, you know, you can block Rachel 10 times from 10 different numbers. They're going to run out of numbers in your black list, as a consumer, to block. And you're just going be listed.

As far about the other question there, I'm really an advocate for industry cooperation. Believe it or not, the industry works very well together. But to Vijay's point, Carrier A, with this small toolbox; Carrier B has a bigger toolbox. Carrier C has a different toolbox. We're not all working with the same tools.

I think every carrier really wants to work together, but some can pull SS7 records, some can't. Some can pull SIP records, some can't. So when you're tracing things back to the network, it may not be because somebody doesn’t want to give you the information, it's that they don’t have the information.

So maybe some standards on what information needs to be kept for fraud management by its capabilities.

MR. COX: So first, what Henning said. This is really interesting stuff, though. It is. It's really powerful. Secondarily, it doesn’t work for consumers today because of technical limitations, a market or a cost or that kind of consideration.

Large-scale business users have different interconnections and have different equipment that's required to do our services.

MR. BALASUBRAMANIYAN: As Henning mentioned, at least as far as what Pindrop Security does, it analyzes audio. It analyzes about 15 seconds of audio and makes that detection. Now, the question arises, is it good enough, at a consumer level, to be able to once you know, let's say a black list of bad numbers, that's one option. And then you know the audio, after 15 seconds there's a little thing that pops up on your screen and says, you know, this call is potentially fraudulent. Is that a good enough device for consumers?

What if you push it further up in the network. The network already sees the audio well before you see it because it's going through that. Can you do something else? At a 15-second level, you can't do very much. Can you shorten that amount enough such that you can potentially start making interesting observations? Or maybe there is a completely different solution out there which actually helps consumers identify this. Is it with industries cooperating with each other, technological solutions coming together? I mean, what you can see with all of this is that this is a really hard problem, right.

So you will have multiple solutions that come together to finally solve it or solve it to a certain extent.

MS. DAFFAN: We have a question that came in by email about what can a consumer do if their number is being spoofed. Wondering if anyone had any advice about that.

MR. PANAGIA: I'll deal with that one because we get that all the time. The first thing they need to do is call their local phone company that’s serving that telephone company and validate with the telephone company, you know, are those calls coming from my telephone company? Nine times out of ten, if it's a mass call event, those calls are not even coming from the local service provider.

What we do in these cases, through some of our industry's forums like CFCA, is we will put an alert out that my customer's number is being spoofed. Can you guys go look at your network and see if that number is coming across or transiting your network and get back with me offline?

What we typically do is we identify -- like if I got that request I'd look at the network. I would look at all the entry points into our network, where that customer's number is coming in and I would try to identify the top carriers delivering spoofed traffic on this customer's number and ask them to cease and desist. I would explain to them, this is my customer's number. This is not coming from my network. I know 100 percent that it's spoofed.

You got to be very specific because some providers just say, oh, our number is being spoofed. You really have to prove that we know this is being spoofed. You need to stop it. And we have been fairly successful at doing that.

MS. DAFFAN: Since we're digging into

technology here, let's really go for it. I have a few questions that are all related about how certain technologies and techniques factor into these kinds of solutions.

One is how does KBA factor in? How can PKI or 1 -- sorry, I don't even know. PKI? PK1?

MR. BALASUBRAMANIYAN: PKI.

MS. DAFFAN: PKI. Thank you. This one I haven’t heard of. How can PKI techniques become useful? And then also techniques like, I think it's RFC 4474.

MR. PANAGIA: I'll defer everything to the smart people.

MR. SCHULZRINNE: I actually know what that means. I will start and anyone can obviously chime in. I believe that PKI is probably Public Key Infrastructure. Public technology, in general, can and should play a major role.

Let me just give you a little bit of background and explain that in a few words. We have a classical cryptography which we are all familiar with even if we don't use it. In the sense of cryptography, namely, you have a secret password, as an example of that, that is used to encrypt or to authenticate yourself to a surface. Only you know that password and your trusted entity on the other side that can provide a password to you. That basic idea has been around for centuries.

A more modern version that is much more recent is a notion where you have a public key cryptography which does something somewhat counterintuitive, namely that you have a public part of a key and a private part, or a secret part of the key. Only you know the secret part, but the public part is published in directories and various sorts.

What it allows is if you sign a message with your private key, the holder of the public key can validate that you, indeed, and nobody else except for you, who knows this deeply secret private key could've possible signed it. You can do that, you can validate that without having specific secret knowledge. So you don’t have to be trusted. It can’t be anybody. You don’t need to know about technical difficulties to make that work, in practice, for a variety of reasons.

But in principle, that's exactly what we need for a number of our validations, namely if you're a legitimate owner of a number, either permanently or you have been delegated that authority temporarily because of marketing relationship, you should be able to obtain one or more secrets of the owner of that number grants to you and receiving parties and parties along the way, such as the carrier, should be able to look at that and say somebody who was assigned that number actually has the authority to release that secret to make that.

So I see that as a long-term solution that requires infrastructure that we don't have at the moment. It requires industry cooperation that we still need to set up, but that provides a technical solution to the number validation problem.

The other problem which was mentioned, which RFC-4474, which is the ability to do, on a less cryptographic level an assertion, a carrier that is presumably one of the good guys, they would assert that this is indeed a good number. As Adam just said, this is my number. I assert, under the usual fraud statutes, I assert that this number is actually validated by me. I have this customer log in, for example, through an enterprise network, PBX or a personal number. I can know that this is not just some made up number and I've passed it on to others. As long as each party trusts the originating party or a previous hop, that number can also be useful.

The problem with that is that it relies on a chain of trust, and unfortunately, that chain has a number of weak links today simply because there is a number of suppliers that let's just say sometimes have either less capability or less desire to ask questions as to who their customers are and what their business model is.

They may not be terribly useful in that transmission chain, but it can help in some scenarios, particularly to identify the good guys when the common case occurs, namely when say, a large consumer, originating consumer carrier provider, whether it be a cable company or be it a traditional local exchange carrier or one of the recognized Voice over IP companies, directly terminates traffic on another one of these entities because then you can say with some certainty say, yep, this is indeed a good number.

So both of those techniques are well standardized, but they still require additional industry cooperation where we hope that ATIS and others will help make those possible.

MR. BALASUBRAMANIYAN: Absolutely. I think the first thing was KBA, which stands for Knowledge-based Authentication questions. If you look at the history of trying to authenticate someone, there are a variety of ways that you can authenticate. You have what you know, who you are, and what you have. So the examples in each of these are, you know, what you know is things like your mother's maiden name and Social Security number.

KBA actually falls into that category. Who you are is things like biometrics and things like that. And what you have is things like your phone device. So KBA falls into the what you know category. So these kind of questions is what a lot of the industry uses right now to identify when someone is calling and whether they're really who they are. So what's your mother's maiden name? What’s your Social Security number?

What’s happened, largely, is that the questions are either too simple, in which case, you know, most attackers know how to get your mother's maiden name from Facebook. It's easy to do that. Many times they can circumvent the question. Like, we had this attacker who was asked what's your mother's maiden name, and he actually said my dad married twice so can I have three guesses? He didn't even understand the question, right.

So it's funny, but when you're talking about knowledge-based authentication questions, the big problem is that you're expecting your call center agent to make that decision of whether he answers the questions right, sufficiently or not, but then the questions start getting harder. What's the third address from now that you lived at? What was the last transaction that you performed?

And you're thinking to yourself was that the AT&T bill that I paid or was it me eating out at a restaurant? So the questions get harder. Then it immediately jumps into a customer satisfaction problem, right. I just don't want to be answering seven questions every time I want to check my account balance.

So KBA questions are good as another area of defense. It can't be your only level of protection. The other thing that was mentioned was PKI, Public Key Infrastructure. Public Key Infrastructure has had a colorful history. But the big thing, at least in the telephone world, is Public Key Infrastructure works if you presume you have a homogenous network.

That is, you have the same network on both ends and they both can communicate with some protocol that each of them understands and every party in between says that they are going to sufficiently adhere to the standard. The problem is in the telecom network, like Adam pointed out with his call flow, is that you're going across so many different networks.

On the PSTN level you have SS7 and the audio.

On the IP level you have SIP (inaudible) signaling and RTP as audio. These protocols don’t line up nice with each other. They throw away everything when they go on to the other network. So the problem is, when you want a PKI infrastructure you presume the infrastructure's homogenous.

You, in this case, have to assume the infrastructure's homogeneous, not only in the U.S., which is well advanced in its telecommunication infrastructure, it's rapidly getting a lot of IP. But you expect every other country to also have that same homogenous network because you get large calls coming international place to you. So PKI can work only if you have some kind of homogenous network or there is some kind of handshake somewhere. Otherwise, you will have to figure out other alternatives to do that. RFC-4474 -- is that P asserted identity?

MR. SCHULZRINNE: Yes.

MR. BALASUBRAMANIYAN: It is. Yes. Okay. Like Henning mentioned, that is proxy-based. That is your service provider essentially asserts your own identity and it gives you limitations as well.

MR. COX: I think I can add some additional value just on a couple of small points. I think most of it was really well nailed here. Knowledge-based authentication, we actually refer to it somewhat affectionately as identity interrogation.

The problem is that with 200 million Americans -- I mean, we all do, right? What’s your mother's maiden name? What’s your date of birth? And so on. Your mother's maiden name is on ancestry.com. There are a whole bunch of genealogy sites. Your date of birth --

(Fire alarm. Brief interruption.)

MR. COX: I don't want to terrify all of you, but some of the folks on the phone, I imagine, are probably the bad guys, I'm going to guess. If I were a bad guy I would be listening to the conference.

Social Security numbers are quite available now because Carnegie Mellon discovered the mathematical formula that was used to issue them by the government. It's published. Google it.

The reality is identity interrogation doesn’t really authenticate you. So we have to look at multi-factor authentication. So the tools that we're providing into the something you have space, turning a phone into a unique credential, combined with information-based authentication, and also biometrics is what provides high quality authentication.

MS. DAFFAN: For those on the Webcast, if you don't know what the pauses are about, there is a fire alarm happening. But we can all ignore them. There's no problem.

There's a question, and it might be one of the last ones we have time for, from in the audience. Can you be more specific about Congress' role in all of this?

(No response.)

MS. DAFFAN: The answer is yes.

MR. SCHULZRINNE: Let me give one cautionary answer. This is probably more for lawyers to speak to as opposed to an engineer.

There is some concern that the conditions under which caller ID spoofing is legal and illegal is sufficiently murky that that makes some approaches more difficult than they need to be. I think that's one way of putting it.

Congress, for example, is... A set of applications- I mentioned a few of those which I think most of us would consider in addition to authorized marketing to business relationships which would probably be considered to be a societal value. But a defense, prank calling somebody, as long as you're not threatening or doing any otherwise illegal behavior, is currently not a criminal offense under that act.

One can ask whether that is the right balance to strike because it opens up a defense for people to make other protections to be part of. So that's the only one that I can think of in this case.

One that was mentioned early on, I think, aligning the penalties. And one that I can think of and you may want to speak more about is to make sure that if we've come up with more automated means of tracing back phone calls that those are not handicapped by paper-based processes which just don’t scale up.

We should be able to automate -- we got protecting privacy and rights of all parties involved, but we should not be held back by the need to provide things of what wax seals to each carrier along the way to trace back, as long we have sufficient privacy and consumer protections in place so that that process itself can be of use, which we clear need to do.

MR. COX: What Henning said.

MS. DAFFAN: So this point about leading to trace-back faster, what other steps could be taken to assist in helping people who need to know and understand where a call came from?

MR. PANAGIA: I think there needs to be training for law enforcement, whether it's local, state, federal regulators. I can't tell you how many times in dealing with local or state law enforcement, I mean, as soon as it goes out of the state they're kind of off bounds. But even on the federal side, you really -- the first thing somebody does when they're investigating one of these things is they subpoena the spoofed number carrier. And that's like the very first brick wall they've had and that's where it ends.

I think what we need to do is trace the records back so that whoever is issuing subpoenas needs to know how to ask the right questions and I think this group needs to maybe put those instructions together so they'd ask the right question so they can go up the stream.

MR. COX: That's a great point. In many cases the carrier is also the victim of that.

MR. SCHULZRINNE: What's really the most important information is, interestingly enough, not who was calling -- not that it is easily spoofed -- but who was being called because that number can’t be spoofed. Obviously you need to reach that. And the precise time when the call occurred because with those two pieces of information, you have much more chance of actually tracing it back, but both of those have to be precise, you know, time precision, particularly if it's a larger call volume and you certainly need to be really sure that that's the destination number that is reached.

MR. PANAGIA: I’ve recently given some instructions to one of the agencies and it is to start at the victim's homes and work your way back because that can’t be spoofed. You know the call landed there. Start there and go back. Don’t try to shortcut it by oh, that telephone number there belongs to AT&T or Verizon and we're going to subpoena them because you're going to go off into a black hole.

MR. COX: Let me add one thing to that. I don't want to alarm you guys, but now we're seeing that that number that's being called can be spoofed. This is scary.

MR. SCHULZRINNE: But how would it reach your destination?

MR. COX: So what happens is, I'm a criminal and I want to take money out of your bank account through a wire transfer. I won’t give all the tricks to it because again, we don’t want to educate people because we need to be non-educated.

In essence, I can socially engineer a phone company or I can socially engineer you to forward your phone to me. So when you think you're calling somebody -- I know you talked about this as well -- you think you're calling a party but you're not. You're getting the criminal. I say yeah, here's all the bank wiring information. We did, in fact, just sell the company. Go ahead and bank wire that $384 million to me. Everything looks good because they've called, right? Because we assume that number can’t be spoofed, but you can socially engineer people. People are always -- we're trusting. Right?

So you socially engineer the person. You forward the phone or you socially engineer a phone company rep, you know, hey, I'm at the office. I'm waiting for a really important call today. I forgot to take my cell phone. Can you forward my home calls to me at this number here? And the rep says, sure. I'll do that. Right? You get the idea.

So, again, all threats that are on the internet today are coming through on the telephone number.

MS. DAFFAN: We have a bunch of other questions, but only time for one more to pose to the panel. It's one from the audience. Would it be useful to have some kind of center that brings together law enforcement and the telecommunications industry in one place to tap all these questions?

MR. PANAGIA: Yes. We have those associations. There are things like InfraGard.

There's things like the NCFTA or Cyber Fusion Units that we all belong to. There are Cyber Financial forums where the financial industry, law enforcement, and telecom are comparing information and trying to help each other because of the schemes that the financial industry is seeing is utilizing the telephone network to get there.

Not many people are falling for the old email stuff anymore because there has been so many warnings out there. Now they're moving to the phishing scams and they're largely telephone number based now.

MR. SCHULZRINNE: I don't know if you want to talk about that, but there are really two parts to that question, namely, on a longer scale that I think is working relatively well. What's a little harder is on an operational day-to-day basis, which is what you mentioned Pat.

MR. BALASUBRAMANIYAN: Extending on that operational basis, I think the U.S. gets about five billion -- I don't know the number of calls that it gets to call centers everywhere. At any given point in time, even if you reduce the number of good calls or bad calls to .1 percent, you're still dealing with 14 million calls. So you have to have technological solutions that can help this go forward.

MR. COX: It's 52 billion.

MR. BALASUBRAMANIYAN: Okay, 52 billion. So even if you do .1 percent of those calls are fraudulent, then you see that it's pretty significant.

MS. DAFFAN: Okay. Well, thank you all very much.

(Applause.)

MS. DAFFAN: We're going to power through here and have a break after this next presentation. Now we have the luck of hearing from David Belanger, who was the AT&T's Lab's chief scientist until very recently, and who is now senior research fellow with the Stevens Institute of Technology.

(Applause.)

* * * * *

DATA MINING ANOMALY DETECTION

MR. BELANGER: Thank you, Kati. So we will go on about potential solutions due to robocalling problems today and a lot about some of the things standing in the way. I'm going to talk about one of the approaches that has been very useful for detecting fraud, robocalling being another form of fraud. I'll talk a little bit about why detecting such a challenge now and where these techniques are going. I don't have a solution to the problem, but if I did I would've probably announced it before the conference.

If you think about the kinds of solutions that we've been hearing about, they can fall into something that is fundamental to the network fabric. Those are challenged by -- network fabrics take a long time to change, especially internationally. Things that are overlays on them and those can work very, very well.

What I found is that scale is the challenge for overlays. We're talking about double-digit billions of calls per day. So scale underlies nearly everything that's done, And a variety of ways of detecting a robocall when it occurs. The techniques that we've been using fairly successfully across the industry for fraud detection is essentially behavioral.

The advantage is that they can deal with scale and they can be implemented, given enough computing power relatively quickly. The disadvantage is that they're nonsyndromic, which means, essentially, that you're not taking a piece of data and saying this thing is a robocall. I know what to do with it. I can trace it back, et cetera. What you're doing is taking a lot of very weak signals and putting them together and saying I have an alert. There is a robocall going on, something of that order.

To give you a feeling for nonsyndromic data -- and actually, I think Kevin Rupy mentioned this effect, although not the specific instance -- you can very often tell from watching a telephone exchange that some event is happening. You can’t tell what the symptoms are so you can’t necessarily tell what it is.

About a decade ago we identified, for example, that there was a very large event occurring in one of the southern provinces of China. Contacted a nearby medical school and were able to determine that it was SARS. Very early on, a leading indicator to this.

So the effect is that lots of very weak signals can tell you that something's happening. You may need extra information to find out what is happening and therefore, in the fraud world you often have fraud control organization much like what Adam has talked about today.

The idea that I'm talking about is to take behavioral data, which is thrown off by the networks, the services, or for that matter these days, crowds. Put it together in a way that can cause alerts to happen that indicate that there may or may not be a robocall occurring and reduce the false positives as much as you can. Now the real challenge is to see if one of them works.

So this is the general outline of what I'm talking about and it's very general in the sense that it's about data mining. It's about data. And the idea is that you have large sources of data, you know, the collection of tools are on the outside. This should surprise no one. And do you have a collection of applications. On the far left you have the managing risk applications, security fraud, et cetera. But down in the lower right, the vertical services, you'll find that these techniques are being used to cross communications, financial industry, the credit card industry, for instance, increasingly in healthcare and energy. So the basic notion of taking behavioral data and analyzing it those sophisticated ways to understand that something is happening is very broadly used.

What I'm going to do is talk about using an example which has most of the stresses of the robocall outbreaks, i.e., it’s not going to be able to work as is, as it traditionally has in robocalls, but it's a simple example. So it gives you a feeling for how 1) fraud might be addressed behaviorally and 2) I'll go through some examples of how in reaction to the fraudsters becoming increasingly sophisticated, the techniques for identifying them had to become increasingly sophisticated.

So where does data come from in large quantities? Well, the network. And we've heard some discussions of whether we could intercept, in real time, robocalling and do something like blockage in real time.

The network has the characteristic that things happen very fast. Things happen at ridiculous scale. So we think a few billion or a few tens of billions of calls a day might be interesting. We're talking about several tens or a hundred billion packets a day, going across a hundred trillion packets a day going across the IP network. A very fast start to get a conflict between how fast you can do something and just how much data is going across there. Often you end up doing things like sampling, but here we're looking for either the needle in the haystack or the needle in the needle pile in the haystack. The haystack is very, very large and moving very quickly.

The second layer, the one that's traditionally been used, is services. I'll use call details records as a stalking horse, but nearly every service throws off a collection of information about what it’s doing, the mobility services due, for instance, they throw off usage so that if you overuse whatever number you have, you can get a message or being charged. Very often these are done in the service of billing and so is data that's collected in any case.

Customer data is also there. I'm not going to concentrate on this because it's really not a significant player in the behavioral instances that I'm looking at.

What are the challenges? The challenges are exacerbated by the characters, such as spoofing and robocalling. But the major challenge is scale. These simply are at the edge of what, and probably in most cases, beyond the edge of what commercial computing can do. It's what's called big data today. Five years ago I've had the same kind of characteristics, but it didn't have a name.

The scale is at the edge of what you'll find in any industry on a given day and commercial products are often challenged to do a day's worth of input in a day. Obvious problems.

The second -- and this one has gotten a lot worse lately -- is integrity of the data. And we've heard a lot about that today. We just can't trust the data in many cases. It's bad enough when the data is intended to be good and it's simply because of its size and mobility that errors turn up. But in this case, it's not intended to be good. It's not coming from a source that you have any control over. So trusting the data is a significant problem.

In this industry, security and privacy are overwhelming issues. Not because we want to get rid of them, but because we want to ensure them. We heard some discussion earlier today from David Diggs about privacy being in the DNA of the industry. It absolutely is. Security is another issue that is a huge challenge.

So a lot of what's going on is taking into account the fact that we are not going to see the content of any of these instances that are going on. We're going to act on information that’s nonsyndromic.

And efficiency.

I can guarantee I'll catch every robocall that's got issues if you'll let me claim that 90 percent of the calls are robocalls. Now, I'll catch a lot of calls that weren't robocalls, too. The idea is to have very low false positives, but very high probability of capturing what you're looking for.

So this is basically a very naive schematic. You saw a bunch of network schematics today. All of those are in that block off to the left. All I'm interested here is in what data is thrown off by that network. That network including other people's networks as well.

There is a whole bunch of data that is sent immediately to collectors and then either sent down for activities like billing or sent to a near real time system. Most of the fraud systems, for instance, for voice are near real time, to analyze in a variety of different ways to see if there is a behavior that is potentially fraudulent and to alarm them.

And then there is the real time activity. The SS7s, the IP packets of the world which have order of magnitude at least more scale than the near real time and order of magnitude, less latency tolerance. It's very difficult to imagine using that data on a whole network basis to do behavioral analysis.

So let’s see what’s going that's changed and what’s going on that's the same in terms of analysis. I'm going to skip over this pretty quickly, but in the top left is the kind of data that you're going to see if you get a call detail record.

Now, unfortunately, we've heard the initiating number may be spoofed. We've heard that the terminating number may be spoofed or forwarded. The rest of the data there may also be impacted. So you have on your hands a collection of data which you have to not only understand what it's trying to tell you, but understand that there are issues with it.

Let's go on to the next slide. I should mention that there are cases such as media-induced events which are nearly the inverse of robocalling, where you have lots of people calling a specific number. So think television voting systems, radio call-in shows, that sort of thing.

On those, you also want to detect whether somebody is robodialing into them or else the results are fairly useless. This is a much more controlled environment with a much lower financial impact. And therefore, certain things are doable in that space. I'm not claiming that proves that we can do something in robocalling, but it's an indication that certain analytic techniques expand very widely.

So let's look at the types of analysis techniques that have been used over the years. In the middle '90s, the way you'd identify fraud would be looking for a threshold.

This person called a certain place for more than 15 minutes, which was probably a foreign call. Probably they don't intend to pay for it. So the effect that you saw was all of a sudden, to that place there would be a lot of 14 and a half-minute calls. The fraudsters are not idiots. They are very intelligent.

Next step, we move to individuals' signatures. And we heard something about signatures in a few talks today. And there, the idea is, is this entity, this communications entity, may be a phone number or it may be something, is it behaving in the way we expect it to behave or is it behaving in a way that it indicates that something strange is going on there? You can do this very simply, actually, at very large scale with very simple data that we showed there, you know, initiating number, terminating number, time of day, day of week, et cetera. A lot of fancy mathematics goes into it, but it can be done simply and at that enormous scale.

Well, what's the problem with this today? The problem in robocalling is that you no longer can trust the initiating caller. So what you can’t base this on is that initiating caller behaving strangely. You could use that and you would probably get some indication of whether the initiating caller was actually the caller you thought it was.

The more powerful, the more recent techniques are based on relationships. So for example, if you -- and now I'm talking about you personally, not you as a robocaller -- had two numbers and they're quite separate and you made a lot of calls. You would probably be identified fairly quickly as the same person with very high probability. Why? Because you're going to call the same network of colleagues in the same pattern. So there are techniques which start to look at getting beyond individuals to more powerful sets.

Let me just summarize a little bit, in terms of where we've been and where we're going. "We" being the industry as a whole, and for that matter, the financial industry and a bit lagging, because of the data available, the healthcare industry.

Starting out with aggregates to aggregates, very generalized data, you can tell, for instance, if there's a problem on the network, in particular, in an area with a cell tower, et cetera, but not much in terms of landlines.

Going from individuals to aggregates, that's threshold. Same value applies to all individuals. Not hard to defeat, and most for us is we're defeated, nowadays. Signatures are much harder to defeat if the individual data is trustable.

Going down further, relational, meaning a graph of numbers, for instance, which are related in some way, can be addressed by graph measures, but more likely in the more powerful instantiations by whether the graphs are with high probability, the same graph or institute of the same entity.

And finally, and not to be ignored or to be ignored only at a peril in these days, crowd sourcing data is very valuable in a lot of instances. Tutor data has been used as a leading indicator to network problems. People see a network problem and see a service problem and start to Twitter about it. If you monitor Twitter you will sometimes see indications that something's happening.

Mark the Spot is an AT&T app. There are probably some more apps elsewhere, but essentially it's an app that says if your cell phone is not receiving service, you punch a button. When it's next on the network it will send a note to the network folks saying I had this problem in this place. It's a way of actually getting very syndromic data in this case.

Now you know there was a problem and you know what kind of a problem it was. It’s reporting at a scale that is beyond what calling a customer service entity is likely to be.

Although not either available or used in this area, the social networking folks have just an enormously powerful set of data for understanding what's happening in the world.

So that's what I wanted to say, though I may have announced the break too soon. My panel will answer any questions that you have.

MS. DAFFAN: So we're open for questions. We do have some questions already. Looking at the network from the point of view where you sat at AT&T Labs or a similar point of view, is there any way to guess whether a call is a robocall before a consumer's phone even rings? And if so, can you talk about that a bit?

MR. BELANGER: So the answer is I don't know of it. We've heard today some indication of technologies that might be applied, either violating authentication or other techniques which involve overlays in the network. In general, you can hypothesize that you would have a way of identifying that the call was from a member of the set that you had reason to believe was a robocaller, but today there's certainly no techniques that I know.

MS. DAFFAN: Can you talk a little bit more, following up about that, about the example when calls are coming in to a particular place. You talked about some kind of, you know, competition.

MR. BELANGER: So if you have a phone call is coming into a specific number, radio call-in shows, television voting shows, et cetera, very often the impact has the effect of being a voice to mail or service attack, but from the point of view from the business buying the number, usually it's an 800 number that these calls are coming in to. They would like to have an accurate view of how many people are calling in, not on any of the machines that pick up the call.

So there are a actually fairly naive approaches to detecting spikes in calling patterns from specific places and specific numbers that would distinguish between how fast you might be able to press button or even press the redial button and what a machine could do.

I think that the difference in robocalling is twofold; one, the techniques being used are much more sophisticated because there's much more money involved and they are targeting millions of phone numbers.

MS. DAFFAN: What are some examples of practical applications of data mining that a carrier might use?

MR. BELANGER: I would say that most of the fraud and security and the network reliability techniques today, most of them are networks, are as being the entire industry are based on data mining. They are based, as you saw, the kind of data that you saw because the actual payload of the call or the pact that's entered is simply not used, not available. But if you were to look at how the network operations alarming systems work or the network fraud alarm existed as security, most of them would be applications of data mining and that sort of thing.

MS. DAFFAN: Do carriers ever block call based on information like data analytics that could come out of a lab like yours?

MR. BELANGER: For the answer to that, you would have to ask Adam, who would be involved in that.

MR. PANAGIA: Yes. Thousands of times a day.

MS. DAFFAN: So what Adam said, for people who couldn’t hear, was thousands of times a day.

So your role is to sort of package the data and send the information on to people like the fraud team?

MR. BELANGER: My role was -- and there are still people in all of the large communication carriers -- was to invent the algorithms that might be able to detect an alarmable event and send the alarms to a downstream team, recalling that. Because this is typically a nonsyndromic data, you don't know for sure that this is an event, or you perhaps don't know how you should react to the given event. That’s what these downstream teams do.

MS. DAFFAN: Related to the earlier question, would there be a way to not know for sure that a call was a robocall but had some kind of an educated guess, maybe a number on a scale.

MR. BELANGER: Zero to one. Yes. The output of most systems which are generating alarms is whether it’s an event or not, a probability that this is not a false positive.

MS. DAFFAN: There's a question here from the audience about where law enforcement can get access to some of the analysis or the relationship data that you've been talking about. I guess how we could pull it together.

MR. BELANGER: I think that law enforcement typically works with the downstream people who have confirmed that it's an actual event of interest to law enforcement. If then there are requirements for more data, it would come through those organizations.

MS. DAFFAN: Is there a way that algorithms that you're

talking about be used to present consumers with an option to block certain kinds of calls that might have a particularly high probability of being fraudulent if the consumer decided that they wanted to take that step, knowing the possibility of false positives?

MR. BELANGER: Well, that's a good idea. Maybe I should start a small company.

The answer is that they would have to be dramatically simplified algorithms and they would have to work based on knowledge of that consumer and that consumer's rule set.

So there is nothing to say that it couldn't be done. The operational characteristics of it would be staggering. A very technical person of the type that we saw a few of from the panels today, probably do it on their own. I don’t think that we're anywhere near having the technological capability to build a generic one that people could simply put parameters in.

MS. DAFFAN: Good. Well, I think with that, we will go to our break and we'll see you back in 15 minutes.

(Applause.)

(Brief recess.)

CALL BLOCKING TECHNOLOGY

MR. BANDY: Good afternoon. My name is Bikram Bandy. I'm a staff attorney in the Division of Marketing Practices at the Federal Trade Commission and I focus on enforcement of the Telemarketing Sales Rule and Do Not Call. I'm the moderator for today's panel.

Today's panel -- well, for most of the day today we've been talking about playing offense against bad robocallers. Law enforcement; how can we find out who they are? How can we go get them? How can we throw them in jail? The quest is to take down Rachel. And that's certainly -- and we've heard a lot of good ideas about how we can be more effective in that and we've also heard about why it's difficult to track down Rachel because she exists in multiple forms and she's hiding very well, often overseas.

What I wanted to focus on in this panel is about playing defense against Rachel and really allowing consumers to do things on their own that would prevent unwanted telemarketing calls from getting through. Really, that's what we've been talking about and what’s been mentioned before is call blocking.

So we want to have this panel talk about what call blocking is, how it works, what its current limitations are and what are some of the things that can be done to perhaps, give consumers more power to prevent their phones from ringing in the first place.

I have talked to a lot of consumers that are very frustrated by these calls and they say, you know, the same person, the same number, or the message I keep getting over and over and again. And if you can just make that one message stop. If I can stop just that one message, you know, maybe I can get to take that nap.

So there's definitely a consumer desire to be able to almost engage in some self-help, and I think call blocking is one of the options. It's not something that you can just wave with a magic wand. There are some issues with it and I think our panel today is going to talk a little bit about it. Let me introduce our panel.

First, to my left I have Andrew Whitt, who is the director of Global Maintenance Engineering Voice and Communications Services at Verizon. He has over 34 years of experience in the telecommunication industry. At Verizon, he is responsible for overall network reliability of Verizon's landline and VoIP services and for supporting Verizon's network evolution to next generation technologies.

To his left is Jeff Stalnaker, who is the president and co-founder of PrivacyStar, a company that provides consumers with mobile privacy protection services such as call and text blocking, caller ID, complaint filing and other privacy-related features for consumers.

PrivacyStar has an application on the market that assists consumers on blocking unwanted calls to their mobile phones that he's going to be talking about today.

And finally, on the other end is Matt Stein, who is with Primus Telecommunications Canada, which is the largest alternative telecommunications company in Canada and serves residential business and wholesale customers with a full suite of telecommunication services.

Matt is going to talk about a product that he invented, which is Telemarketing Guard, which is offered to Primus customers that helps block unwanted telemarketing calls. So that's the panel. I wanted to start off by having Andy talk a little bit about what call blocking is and how it works in its current incarnation, particularly on legacy landline networks, what its limitations are.

MR. WHITT: Good afternoon. First of all, I would like to thank the FTC for putting this summit together. As I've sat in the audience throughout the day, the speakers and panelists that have talked throughout the day, what a very distinguished group, very much the right people to be here to talk through this very specific issue.

So as we begin, in terms of this particular panel and kind of what we wanted to focus on is what can customers do now. Throughout the day we heard, it kind of talked about at the beginning, way back when. Today we've heard a lot about what the future might hold and many of the problems or challenges. What I'm going to focus on from a Verizon perspective is what do we have now. What’s available now? In some cases I think it might be fairly basic. Some old tricks, if you will. But just to make sure everybody understands what those capabilities are.

Just to frame up conversation earlier, again, you've heard about it and I'm not going to bore you with redundant discussions about the PSTN, but that is a large part of the network, not just the U.S., but, of course, internationally.

I think the key point, as was stated here is that there are some limitations. We as providers, AT&T, Century Link and others use very similar technologies from various vendors. Over the past 30 or

40 years, the industry worked together to identify features, functions. Just a few years ago Bellcore was a key industry driver. So in some ways it was build it and they'll come, relative to some of the services, but clearly today, the market drives that, which is a good thing.

As some of my fellow panelists will talk about today is some of the solutions that have been enabled by competition and market-driven solutions. So again, limited technology in the existing switches, they were designed and implemented several years ago, long before the iPad and iPhone, et cetera.

Broadband services are very, very much the future. When you think about the different technologies, and I listened for it, but I didn’t really hear a specific kind of clarifying statement because if you think about wireless, VoIP, landline, you mostly are talking about the access technology, when in the core, it's actually migrating to VoIP as a core network, but still mostly, that legal circuit switch, or we might say TDM, time-division multiplexing core.

So broadband services, ultimately, for us as a business, and also for our customers, provides a brand new infrastructure for a lot of great innovation for the bad guys and for us. So it’s kind of an arm's race as we go forward.

In terms of wireless -- I'm sure everybody is on the same page here in terms of wireless, it's really then the driver in evolution of this network. As we migrate that core network to a thing called IMS in the near term. We're going to get to a very standard-spaced infrastructure that's going to really help us as we begin to look more deeply into solutions to expedite, if you will, the identification in addressing those robocallers and other nuisance.

In the end, I would just say from our perspective of providers today -- and it was said a couple of times, but I think it's important to say it again -- we want to complete calls as an industry. We want to complete a call.

A call comes in and unless it's very much apparent or customers have complained, we’re going to complete that call every single time. That's the expectation of our customers. That's the expectation of all of our various regulatory agencies.

So completing calls is very important to us, but also that privacy. I say that again because when I started 34 years ago, the very first thing I read was how quickly I would get fired if I ever told anybody about a call being made, who called who, what the content of that call might've been.

Privacy of communication -- again, DNA was a great term earlier -- is very, very important to us. That could be a bit of a challenge if you're trying to figure out or distinguish a good call or a bad call. Ultimately, it comes down to customers telling us, giving us that intelligence.

So everybody had a network drawing, so I had to have something. This is really, really basic. I like to make things as basic as I can. The reason I'm showing you this, very, very quickly, is that the old technologies, those old switches, those wonderful things that we installed when I was young and new in the industry were very much a big box. They were very monolithic. They were proprietary. They were coming from big vendors, so everything was together. We have lines to our customers. Remember earlier, one carrier and one pair of copper wires, right? Then we had trunks. We heard trunks earlier, interconnecting our end offices with carriers and international gateways. And then in the middle is that wonderful switch fabric. When I first learned about time switching I thought this was pretty cool. Again, it was a matter of current technology 30 years ago, very advanced.

That service logic, key point is that it was right there locally in the machine. In our network are thousands of these machines in our network at Verizon or AT&T, Century Link and others. So this is the network. Still, in many cases, this is the machine providing dial tone to our customers. When you think about that old technology, again, I just want to take a few minutes and focus on what is available right now. We talked about call blocking, but let's be clear, before you block it, you got to screen it and we want to give you some opportunities to screen it. That's really what caller ID is, right? It's a screening technology. It gives you some awareness.

Now, I don't know about any of you, but have you ever put an address in a GPS unit and you follow it blindly until you get to that dead end? Now, I didn't throw the GPS away, but most times, probably 95 percent of the time it gives me the intelligence that I can make the best decisions to get to my point of destination. Same with some of these technologies. As you heard, because of spoofing, because of some of the advanced technologies, caller ID sometimes isn't accurate, but most of the time it is.

Just about 15 years ago I thought, you know, when you're on the call talking to someone on that landline, we used to share a little tone if somebody wants to talk to you. We added caller waiting ID so that you could actually see the person who was calling while you were on that call to give you the decision, again, a decision point of should I take that call.

Now, there has been some talk about anonymous call rejection. It's actually a pretty good service. Now, it's not as effective with spoofing, but we do have a lot of providers, or I should say bad actors, that will block their caller ID and the network can identify that and route them to a message saying listen, if you want to call me, you better unblock and give me your identifier, right. It's a nice feature. When that was designed, it was an incredible advancement, but that's before the advent of these kinds of robocall type technology.

Call block, as an example, *60 is pretty much an industry code to use, but I would very much check with your provider. Good news there is that you might get a call in that says blocked and you picked it up and if it was abusive, you could *60 and put that caller on a block list even though you didn’t see the phone number because that phone number is known by the machine.

I think call trace is something that doesn’t get enough air time, so I wanted to make sure we talked about it today. We, as an industry, as was said by Adam at AT&T and many others, we work together, but more importantly, we work very closely with our law enforcement agencies at local, state, and federal levels.

What’s nice about call trace is that in many cases it’s a pay per use. You don’t have to subscribe for it, just *57. As soon as you do that, when you've gotten an abusive call, *57 records that in a record that can be used in a legal proceeding to prosecute. We don't tell you who called, especially if they're blocked because we can't, that's the rules, but when you call Verizon's Unlawful Call Center, then that is how we can initiate, work with, reach out to our law enforcement agencies.

So at the very bottom of the page, there is a little link there to talk about some of those call features. Again, I would say that folks should always read up on your providers, in terms of those kinds of capabilities.

Again, just another real basic view, it kind of blew up the old network, if you will. You got that VoIP in the middle. That's where we're heading. We're heading to a VoIP infrastructure. Notice we no longer have line cards, we have gateways.

A really good point made earlier was that as you transition through gateways you lose context. You lose some of the key intelligence that we would've relied on in the future.

Simply, the point is that VoIP is a great thing, but it can, of course, provide some capabilities for not only us as providers to give new services, but also the bad actors to leverage that.

Talking about Verizon, we have a service called FiOS Digital Voice. On our landline network we have fiber. And over that fiber we now have a VoIP service called FiOS Digital Voice. The nice thing about it is instead of just using your handset and those tones to activate features, et cetera, now you can go on the website or you can use a smartphone and you can identify and track your call log, message block list.

Of course, many providers now, equivalent to FiOS, can be sitting at home watching the Super Bowl and that call comes in -- what's nice about it now is with this service we have called Voicemail Stream, again, a screening feature, you can pick the phone up and wait until the identifier shows that it’s going to voicemail, go off hook and listen to the caller leaving a message. It's a screening capability so you can say do I really want to take this call?

It's kind of like the old-fashioned answering machine, which was a really great screening device itself.

I just wanted to mention that we've got a very robust business VoIP infrastructure, also, and we do have customers that are autodialers. And hopefully most of the time they're the good players, but when they're not, of course, we again work with those customers to address those bad actors.

Finally, in terms of our evolution, we are, right now, migrating from old technology. Just this year we finally removed the last 1A switch off our network that had been there for 39 years. So we're going through that process. We're evolving that network and we're replacing it with brand new technology that is VoIP-enable northbound to the network.

Real quick, while I just have a minute left, in terms of wireless -- again, as I said earlier, wireless is really driving the evolution of the network, quite frankly, and there's an app for it. It was said a couple of times today. The intelligence in that former model was at the core and it took months, maybe years, to make changes or evolve, but now we have apps, and there's an app for that. There's an app for call blocking and call streaming. You can go on any of the Android market or iPhone app store and there are many applications out there. That's a beautiful thing.

When we think wireless, when you block a number, because wireless can give you text messaging, video messaging, picture messaging. The neat thing now when you block a call on wireless, you're blocking all that, not just the audio. So that’s an interesting expansion of the capability.

Finally, we use, work with Cloudmark. I gave the URL so that you can get more detailed information, but the key point is if you get a spam message and that spam text message clearly is a spam text message, you can forward it to 7726. What's nice about that, like other similar services, it begins to create an intelligent database and as more and more people forward those messages, to connect the dots, we're going to start to block those kinds of messages coming in from the bad actors.

Finally, I just want to say that Verizon, as I've said many times today, we partner with government and industry. Ultimately, working with organizations like ATIS or the CSRIC, which is part of FCC and other organizations like FTC also, as an industry, we are driven to provide those solutions. And as we work together as an industry, we come up with very good solutions because that's what we've been doing for many, many years.

Today, a key piece is that we do have mutual support and that's been part of DNA, in terms of when we have a robocall incident and we reach out to AT&T or Century Link or other carriers, we have our partners to reach across. I like the Batcave idea. I think that would be pretty cool.

Ultimately, sessions like today, probably the most important thing is awareness, consumer awareness. Understanding what the problem is from green, yellow, to red calls and what is available now and understand that it's not going to be fixed quickly, but we're on a path of some pretty amazing solutions. Thank you.

MR. BANDY: Now Jeff is going to talk a little bit about the product that his company, PrivacyStar, has developed.

MR. STALNAKER: I was hoping Andy was going to give me a plug when he started talking about mobile applications, but he didn’t do it.

Let me just start from the beginning. My name is Jeff Stalnaker and I'm the CEO of a company called PrivacyStar. We are a mobile platform smartphone capability to block calls, not just robocalls that we've been talking about all day, but it works on mother-in-laws, girlfriends, et cetera.

We are located in Conway, Arkansas, not Silicon Valley. I get that question a lot. In Arkansas, we're actually pretty smart. We actually created a technology that works. Always got to start with that.

We started this thing in 2008 and we started with the focus on landline call blocking. So we know the two reasons you get rid of your landline. The number one reason is cost. Sorry, Verizon and AT&T. Number two, telemarketing calls. So we know it’s a massive problem. What we figured out quickly, after going to several undisclosed and unnamed carriers who are potentially in the audience, we quickly learned that the technology is 39 years old.

By the way, did that switch work when you pulled it out? Hopefully it did. The reality is that technology is not where it needs to be. By the way, you've got to laugh at some of my jokes here, okay. It's the end of the day. They put an old CPA up here just before you get to go have beer.

So we started this thing focused on landline, but we quickly learned that wasn’t going to work. At the same time, we quickly realized that a lot of people are getting rid of that landline. What happens when you get rid of that landline? You use your mobile -- it’s okay; shout it out if you know the answer.

You use your mobile number for everything. It goes on your business card. It goes on the side of your car. It goes on your email signature. What happens every time you put that number out there? Shout it out. Telemarketers can get a hold of you, either correctly, incorrectly, legitimately or illegitimately. Then what happens? Your cell phone begins to ring.

When we started this in late '08, early '09, I would go and talk to people and they would say I never, ever get a call on my cell phone from a telemarketer. That's what they would say. You guys are wasting your time. You do the same survey now, most people get anywhere from seven to ten per month. And if you don’t have a landline, it can be well into the 20s per month of telemarketing calls. The other thing that hasn't been mentioned here that we should talk about is the reality is that people don’t know that they really should register their mobile number on the Do Not Call list. They should do that.

We find more and more people when they come into our system and use our service that they're not registered. But, boy, they want to file complaints. You can’t file a complaint unless you're on the list. So we have a automated process that tells all of our users that when you try to file a complaint, and even when they register, you need to sign up on the Do Not Call list.

I'm going to get started. Really, what we do, as I mentioned, we have a number of features. There are 14 features that are available. We are available in Google Play. So if you have a Google phone and you want to go out and find PrivacyStar, just hit the search button and type in PrivacyStar and it'll take you about 30 seconds to download, register and then you can start blocking calls and text messages. We are working with many operators. We find that that is better for us, in terms of distribution.

Very importantly, Andy, you talked about the reporting on the 7726, when we started this thing we only had three features to block phone calls -- and I'll talk about this more in a minute -- you can be able to file a complaint with the Federal Trade Commission for Do Not Call and also FTCPA.

However, we got the question all the time, Jeff, that's great, you blocked my ex's phone calls 37 times, but she sent me 105 text messages. What are you going to do about that? So we also offer you the ability to block text messages.

As I mentioned, very, very easy, right after you block a phone call -- and yes, you've got to get the first one. You don’t have to listen to them, but right after you get that first call it takes you just a second and we add it to your block list. Next time that person comes in, your phone won’t ring. It won’t buzz. It won't vibrate. You won't even know that it happened unless you're looking at your screen.

We use technology in the handsets. So we actually execute an answer and it will hang up immediately in subseconds. Again, unless you're looking at your screen, you wouldn't know. What’s very, very cool, though, right after you block that number, we pop up a little window that says hey, would you like to also file a complaint? Boom. You say, "Yes." You can say "No." You don’t have to file a complaint. We're not sending in complaints if people don’t want it. This is a user, a consumer that's making this decision. So we ask, is it a telemarketer or is it a debt collector? Real simple. Then we ask if you would like to provide other information, such as if it was prerecorded, a robocall, it was abusive, et cetera, et cetera.

Surprisingly, about 45 percent of the people that file complaints take the time to fill in those boxes. Over 20 percent of them take time to use the comment box. I always say this; the American public is not at a loss of interesting expletives around telemarketing and debt collectors. They like to use words.

We've actually filed with the Federal Trade Commission around 350,000 complaints in the last 14 months. That's a lot of complaints. We're averaging somewhere between 20,000 and 25,000 per month. We're getting ready to turn on one of the top four operators in about a week. So get ready because the 20 to 25 is probably going to 40 or 45. I think I saw David in here earlier, so get ready for it because it’s coming.

As we turn more and more of these operators on, you will see more and more of the complaints. There's no question that consumers want to file complaints. Some of the challenges we spend all day talking about this, the spoofing problem, it is a problem. We talked a lot about technology. I'm not an engineer. I'm just an old financial guy, but I got it. It's hard to stop it. It's no question challenging for us to fix the problem. I don’t think we'll fix it anytime soon. It's going to take some time. These guys are smart. They change the numbers.

One of the complaints we get about our services is I want ABC Company blocked. I've got nine numbers on here from the same company. Can't you just block ABC Company? Well, I wish I could, but I can't. I was mentioning earlier about the number of blocked calls, about 13 is the average number that our users have blocked. We do have a lady that has 327 blocked numbers. I don't know why she has 327 numbers blocked, but she does and we block them all for her.

Definitely, the call blocking challenges in today's world, you know, if we wanted to fix it, if it wanted to be able to block more than six numbers on some of those legacy switches, you could do it. It can be done. It would take time and it would take money, but it definitely is doable. The VoIP switches make it so much easier. These soft switches are just fantastic. They're like little computers that cost a lot more than little computers, but give you infinite flexibility for call blocking, et cetera, et cetera.

I think one of the solutions is make it easy for people to tell the Federal Trade Commission and the FCC that something's going on. I mean, people love to tell you and us something happened and we want it fixed. So make it easy. Empower the user and the consumer. Our complaint filing capability is just a mirror of what you can do at donotcall.net. It's exactly the same. What we did was when that consumer gets that call and you're angry, that's when they want to file a complaint. Boom. Blocked and filed. I got them.

I get this question a lot: Jeff, I blocked this number -- this is something for you, Andy -- I blocked this number but I would also like to block it on my wife's phone and block it on my home phone. Why can’t I share those?

The other opportunity we have is a service called Smart Block. I know Matt is going to talk to you about this service as well, but this is crowd-sourced. So we reach out to all of our users twice a week and we give the top 25 most blocked numbers. If you want us to and you select Smart Block in your user settings, we'll block those guys.

Now, admittedly, I probably should not say that in this city, but right now the top three or four or political survey companies. It's sort of fine. It's okay to laugh, but a lot of calls are being made, as we all know, and our users are simply blocking those calls.

It’s typical debt collectors and it’s typical telemarketers. It's usually about 60/40 and it's the who's who of those companies that we all recognize that are on the list. We do change it out twice a week.

We are looking at expanding it. We had some meetings yesterday with you guys that we're thinking about expanding it to maybe 1,000. Why just 25? The bigger you can make that list, the more of the standard telemarketing calls you're going to block. You're really helping the consumers who don’t want these calls. This is real simple.

We talked a little bit about technology, the evolution. That's happening. That's good news. No more 39-year-old switches. Although, there will be other problems with the new switches, but that's good. You have LTE and you've got RCS that a lot of operators are looking at. Of course you've got VoIP and IMS. There are lots of cool technologies that are frankly going to help us be more standard in any event.

I guess I'll end with the last point here that whatever technology we throw at it -- I think somebody said this earlier -- the scammers, the spoofers, the fraudsters get access to some of that same technology. So we have to do a better job of trying to stay ahead of these guys but know that they've got access to the same technology. Thank you.

MR. STEIN: Hello, everyone. I'm Matt Stein from Primus Canada, and I'm going to talk to you a little bit about Telemarketing Guard.

First, very quickly, obviously not about robocalls, but who is Primus Telecommunications Canada, and frankly, why are you here? We are a wholly owned sub of the New York Stock Exchange, listed as PTGi. We are a Canadian full service telecommunications company, but we are purely an alternative. We're not incumbent anywhere. We're not an ILEC in any region and so forth, but we're in Canada. It’s pretty big; 99 Points of Presence and we serve over a million customers. We serve residential, business, wholesale, you name it. There's a little list of our services up there.

Telemarketing Guard, I guess is what I'm here to talk to you about today. This was really our initial aim to deal with the telemarketing situation. We had customers complaining about telemarketing. At the time it was a lot of talk about the Do Not Call List and so on. In Canada, we're trying to resolve it in our own way. In Canada there is a Do Not Call List as well.

At Primus, we had a bit of a different

approach and that's what we took. In 2006, and ultimately patented and deployed in '07, we brought our product out to market, this Telemarketing Guard solution. Today, it stops millions of telemarketing calls and robocalls, which I view as a type of telemarketing, with no involvement by the customer. There is nothing they need to do. They need to install. They don’t need to reach out and select their list of telemarketers. They don’t need to buy a piece of equipment and put it in their home. They don’t need you to do anything at all. Without doing anything, we were surprised to find that we had absolutely no complaints from customers that use it.

So we now offer the service as a free ongoing service to our traditional copper pair home phone product customers -- you know, the normal plain old home phone -- and to our Voice over IP customers.

Really, what is it? What it is, is something that lives deep inside the network that when a call comes in to one of our customers, the call before our customer's phone is rang, the call is interrogated and looked at, such as where did the call come from. What caller ID did it come from? What ANI did it come from? How many other calls came from that caller ID or ANI recently or ever more before, or to this customer before, or to our base before? And there are many, many things that are looked at right across the board and it decides, well, based on all this information, everything I know about who's calling and how they called and when they called, and instance of calling and all that.

I'm going to build a score, a live, real time view of the probability that this is a telemarketer and it comprises and builds those numbers. Then it takes that information and it compares it to the willingness of that subscriber, which we assume everybody is somewhat willing to take a telemarketing call. We compare it to the willingness of the subscriber to receive that call and then decide either to pass the call onto our subscriber or to impede it. I'll explain that in a moment.

The customers can configure this if they choose to. There's a little phone interface that you can touch-tone dial into the IVR and change your configuration or you can go to a portal and you can change it there, graphically, but you don’t have to. You can just leave it to run and it runs pretty well.

So what happens is if it is a telemarketer and we decide we're not going to pass that call through, we don't block it. We are a phone company.

We believe our job is to connect the two parties. We're not going to block it, but we are going to screen it. So the network answers the call and states -- and it's in this very complicated diagram -- the party that you're calling does not want to receive telemarketing calls. If you believe your call has been stopped in error, please press one to record your name so that your call can be announced. Well, telemarketers don’t do that. Certainly robocallers don't, but telemarketers tend not to press one.

So typically, the call ends there, in the case of a telemarketer, but sometimes they do, they press one and they announce, "This is Bob's Bait and Tackle." The phone rings at my customer's premises. They answer the call and it says you're receiving your call from Bob's Bait and Tackle. Press one to accept the call or two to reject this call. We then use the fact that that they pressed one or pressed two to further influence the score that that party has with us and, hence, go to our gray list.

First, we're using information about the number of calls over periods, over many different timeframes that this caller, the caller ID, the ANI and so on, have ever called before. We use the fact that it may already be on the black list of some of our customers.

Customers may have already have said, no, that was a telemarketer. You missed that one. I dialed *44, the special star code, to report the telemarketer. We use that information as well. So we've built up an enormous array of information about calls that had ever happened before on our network, across the very large base of users across a long period of time and it compromises to do that.

We also use the fact that on the other hand, we may reduce your score if the caller ID has never gone up before; we've never seen it before. Or, for example, customers in a short period of time have added to the white list. So I have shown here for specifics that we use, but there are about 75 things that are comprised to build that gray list on the fly. So that information is streaming in from all sources. We use the fact that it may be an improperly formatted phone number, not enough digits. Phone numbers don’t normally have six digits. There's going to be seven or there will be ten or it'll be longer. But if it’s longer, it will start with a valid country code and all these sorts of things.

We use the fact that if it's a local number, well, then it should be in the local portability database and things like that. So we have a lot of different things that we've built in to thwart spoofing and so forth that we just included within this.

As for the end-user value -- and I'm going to try to go quickly because I don't want to run on too long -- first off, dramatically fewer telemarketing calls. On average, a reduction of 20 per month per customer in reduced telemarketing and robocalls. So if you think in terms of business days in a month, it's a pretty substantial reduction. That again is average. So there is some hope to get it much better than that.

Furthermore, these announced calls invite the customer to take further action. They engage the customer immediately. We've stopped the telemarketer from calling you. What would you like to do about it? Engages the customer and makes them feel responsibility to participate and to report telemarketers through *44 and the portal web interface and so forth.

Customer satisfaction with it has been fantastic. We noticed a material change in customer churn after deploying it, whereas, we used to experience industry-consistent churn, that dropped very quickly. From a carrier standpoint one of the biggest things that we can do to affect the overall profitability of our company is to reduce the reasons that people would ever want to leave our service, obviously. This became a very big reason the customers wanted to stay. They formed a Facebook fan club. It was a very unique experience back in '07, '08 to announce this product and have that kind of response. We're used to launching things like call waiting and stuff.

We got one laugh. I'd given up. I thought there weren't going to be any. So the user does have the option to change it. They can tailor their settings. They can modify it a little bit. They can remove it. They can do it. But the key to this is they don’t have to do anything. They don’t require the interaction on a regular basis. If they make no further interaction, it still continues to save them time, give them their dinner hour back, so to speak.

And lastly, and very important from my standpoint, is going into this, while designing it, a big concern is where to get that list and really who's going to apply that value to it. Is that a telemarketer? Well, it's charity. Really, that's not a telemarketer. That's different. What about this and what about that?

We felt this way by never putting in one ourselves. Only letting our customers decide and requiring a large number, many, many customers to actually have to report a number before we would consider it a telemarketer. We sort of took that wisdom in crowds approach. If all these people thought that was a telemarketer, who are we to argue?

I will tell you that there was an interesting conversation with our director of call centers when we found ourselves on that list. Change your number; we're not taking it off. And, in fact, we did not. We did not take ourselves off that list.

So where are we now? Telemarketing is still growing. Even to a base such as ours that has for a prolonged period of time been nearly unreachable by telemarketers. Telemarketers continue. They persist. Now, I'm talking about telemarketers and I know here today is about robocalls. I'll play the Canadian card and say I think that's similar. But telemarketing and obviously robocalls are dramatically increasing, even when they're not reachable.

There's been a lot of talk today about do you press one or do you press two. Do you answer the telemarketer? Do you talk to them? I can tell you and I can show you a mountain of data that says that as soon as the call is answered, the robocaller will stay on the phone for as long as you let it stay on the phone. So it's incredible.

I mentioned our little Facebook fan page. I talked about the fact that millions of telemarketing calls are screened every month. And lastly, just on a final note, customer surveys that we did initially were very strong in terms of the enjoyment that people were getting from it, how they appreciated it and so on. And it has continued.

Despite the fact that we haven't marketed it in quite some time, we still have customers that come to us through word of mouth and come back to us. The comebacks are the best. When they say I switched away from a service four months ago, I can't handle the telemarketing, let me back in.

In closing, I guess I'll just mention that we have taken this technology and recently we have begun to license it to other carriers. So hopefully you'll start to see it with some other carriers soon, too. So thank you very much.

MR. BANDY: Okay. We've got a lot of good questions. We'll start with this one. This one is directed to both Matt and Jeff. Can a customer white list phone numbers that have been blocked by your system -- talking about your Telemarketing Guard and your Smart Guard -- as part of a block?

So if someone is on the list and is going to be walked through the normal process, is there a way to say, you know what? I kind of want to hear from that particular marketer?

MR. STEIN: In our case, the short answer is yes. Remember, we won't block the call from reaching the customer without screening. And by presenting that prompt, the person who is actually calling will press one and announce themselves, they can still get through. In a case where our customer is aware that a certain caller or the caller ID, ANI, et cetera, or caller ID specifically, does want to reach them, they can do so either through web interface or through touch tones, they can just have that number on their personal white list, which is limitless. They have a black list as well that is also limitless, so it's a limitless list.

MR. STALNAKER: With PrivacyStar, we currently don't have a white list capability, but it probably is one of the top two or three requested features, in particular as you go international, to avoid some of the potential roaming charges. So we will be rolling that out probably within 30 days. Again, it's been one of the most requested features.

I guess maybe inside that question also is when we go to carriers -- and, Matt, you'll appreciate this -- one of the common questions I get is, Jeff, we don't want our customers to be able to block our own telemarketing. I can't imagine that, but we've never agreed to do that. So I always tell the operators that if they don’t want to hear from you, you're probably wasting money. So we don’t restrict it. So if you want to block your carrier, you can.

MR. BANDY: Here is another question that I think is related to Matt and Jeff. Do you have experience with callers complaining about some people who are actually trying to connect calls getting false positives and getting blocked?

MR. STALNAKER: I think for Matt, for Telemarketing Guard, maybe someone keeps running into the voice prompt menu and they say you know what? I'm calling from overseas and I keep running into this. Or for whatever reason I keep running into that and it's starting to be a drag.

MR. STEIN: I think we've had a few in the five or six years of people that have contacted us and said why am I being stopped? I don't think I'm a telemarketer and so on. Our response has always been the same. We never decided that you are a telemarketer or decided you weren't, and we're not going to change that now.

Our customers, a large enough number of them thought you were so it's not our call. At least in our case, those numbers age off. If nobody is reporting it, it will ultimately age its way back off that list and we just sort of explain how the system works.

MR. BANDY: If a telemarketer or someone who is calling you gets through the voice prompt and then the customer accepts the call, does that number go on the white list automatically?

MR. STEIN: Well, yeah, for that user it does.

MR. BANDY: Okay.

MR. STEIN: For the person that called it does, but we also use the fact that yes, they were screened as a telemarketer, but somebody said yeah, I do want to talk to them. That's almost a vote of confidence. So it also heavily impacts the overall scoring that's done every time a call comes into the network.

MR. BANDY: So for an individual customer, if someone calls them and they get blocked and it's someone that customer wants to talk to and they say yes, I want to talk to that person, that person is not going to get blocked again when they're calling that individual customer; is that right?

MR. STEIN: Correct.

MR. BANDY: But then I guess your system is set up that if you've got lots of people saying I want to talk to this person, then that person may --

MR. STEIN: Well, that's a whole bunch of people almost giving that vote of confidence to that one telemarketer and then that score start to come back down. That gray list score starts to come back down and then that accelerates with age and so on. And then all of a sudden there's screening again until people start blocking it again.

MR. BANDY: Now, Jeff, what about with the Smart Block? Do you have the same problem where people are saying hey, I can’t get through?

MR. STALNAKER: No. We really haven't. It's a great question and I've been asked that many times. As we consider taking that list to 1,000 or maybe 5,000 numbers, I think maybe there is that potential, but I think it's worth it to see if, in fact, we see that come up as a question.

I wouldn’t have anybody calling to say hey, are you blocking, you know, we're trying to do telemarketing to all your customer and they've got us blocked. Nobody has ever asked me that question.

MR. BANDY: Okay. This is a question for

Matt. How good does it feel to make telemarketers press one or two to get through?

MR. STEIN: It feels fantastic.

MR. BANDY: Another question is, are any U.S. companies offering something similar to Telemarketing Guard? If not, is it because of the patent? Is the patent preventing other carriers from offering a similar type of solution?

MR. STEIN: I'm not familiar with any U.S. carriers. I'm not familiar with any other carrier anywhere offering it. Like I said, we are licensing it. As for the reasons, I would assume it’s the patent or perhaps -- well, I would be speculating.

MR. BANDY: This is a question for everybody. To what extent, in your opinion, is a federal regulatory role a) helpful, and b) necessary in combating illegal robocalls?

If so, how and what ways specifically?

MR. WHITT: As I said earlier, I think that it is the partnership between industries, but even specifically federal regulatory is actually very critical when you think back to that spectrum of calls from the green to the yellow to the red.

When you get into that red category where it’s abusive, it's illegal, if you will. We do have to have regulation that gives the industry, gives enforcement the tools necessary, you know, that automatic subpoena on one slide today, that would be wonderful. When we have an issue, we usually, almost always find the bad people, the bad actors. It just takes a while.

So I think it can help us to make sure that FCC in their notice of apparent liability process is quite effective. I think there needs to be some of that, if you will, teeth in the regulation so that when we identify those bad actors, we make it cost-prohibitive for them to continue their activity. We’ve got to be punitive to the level that shuts them down because right now the money is too easy.

MR. STALNAKER: I absolutely agree. I mean, we love the FTC and the FCC. I just want to make sure you guys know that.

MR. BANDY: I'm a fan, too.

MR. STALNAKER: Yeah, I thought you might. Without question, we need regulatory involvement and we need it at the federal level. We've got a massive problem here. If anything, you guys probably need some more attorneys. I can’t believe I said that, but yeah.

MR. BANDY: You're really sucking up to me now.

MR. STALNAKER: Yeah. But all kidding aside, this is a massive problem and it's been a massive problem for 15 years. The DNC rules and regulations did a fabulous job of moving the needle. We have, unfortunately, got a lot of people inside the U.S. and even more outside the U.S. who don't care about the laws and they don’t care about the rules. We've got to go get them. I think if we can create some enforcement actions, leverage some fines and penalties, maybe one of these guys will say maybe I better not want to do that. So, yes, absolutely.

MR. STEIN: Certainly I'd be offering our Canadian perspective.

MR. BANDY: Sure.

MR. STEIN: So I don't have much to say about the FTC, although I'm sure it’s great. CRTC and regulatory involvement in general, obviously it's very key. The only tool that I have found to combat telemarketing robocalls is technology. Technology alone is very powerful, but it's a bit equal. It becomes an arms race. I'll have better technology and I'll have a really great way to detect and they'll get better, back and forth and back and forth. It’s a big enough problem that it obviously needs to be a more sweeping regulatory issue.

MR. BANDY: Speaking of the technology arm's race, have you seen telemarketers make adjustments of how they place calls to beat your current technology?

MR. STEIN: A little bit. We've seen a couple of small things. Nothing major. Again, I would be speculating as to why that is, but there are very slight changes.

MR. STALNAKER: I hate to say this because it may be giving a hint away, but it's really pretty easy to start making robocalls. We've been talking about it all day. It's even more challenging for the carriers because of technology.

You can get a software package, buy a Go Phone and get up and running in probably less than 20 or 30 minutes. And when the carrier catches up with you or the FTC catches up with them, what do they do? They just throw the Go Phone away and go down to Wal-Mart and buy a new one. It's a really, really challenging environment and that's been created predominately by technology. It's the arms race question.

MR. WHITT: So I have the same kind of comments. From personal experience, being in NOC operations for many, many years, we have seen this problem expand. We have seen strategies, very clear strategies, in terms of the bad actors making choices.

We had a really good panelist earlier talking about, you know, Brad was talking about the service that they provide. It's a good valid service in terms of autodialing. We have customers who are autodialers. I think the real key is there is a lot of those providers out there and many times, unless you're very diligent, as was shared earlier, to listen to those messages and do some of that analysis before you turn on the switch and go, we have seen where a particular attack -- and I like to use the term "attack" because that's what it is -- as we begin to become aware of it. You shut down this portal and it pops up over here. You shut down that portal and it pops up over here. So it's a race, very quickly, it's a race in terms of identifying.

Now, at Verizon we have some proprietary tools that when there's a particularly abusive attack, we can turn on some features that allows us to manage it more aggressively across the network, nationally and internationally, but again, that's a process that takes investigation. It takes time, but of course, we're bound by things like completing calls as a primary objective and not just arbitrarily blocking it. So yeah, they are getting more intelligent and their strategies, tactics are getting more complex.

MR. BANDY: This question relates to sort of the existing call blocking services and a little bit to Jeff, probably, as well. Is there any reason why I should have to pay extra to block or report an illegal robocall?

I'm already paying for a service. Shouldn’t my local carrier do more? I wanted to see if you wanted to address the money issue.

MR. WHITT: Well, I'll attempt that. Again, from a non-operations perspective, we have features, as I shared, in terms of wireless. Verizon Wireless gives you five numbers to block. It's not an extra charge. You know, you can block those numbers, but it expires after a certain amount of weeks. But then for a premium, of course, we can do some extended block for a greater period of time.

So I think at the end of the day, it's a market-driven economy. It's a market-driven industry. So clearly, as we have to expend resources, especially in older technology, it’s very possible to put in place these services and features and to recoup that cost through some of those extra charges.

As an example, many things are paid per use, as I said earlier. You don’t have to necessarily subscribe to it, but if you will become a potential victim, you can utilize that service one time. Do your *57 and do that call trace. You don’t have to subscribe. There is a little charge, but you think through that, you know, we've got an organization called the Unlawful Call Center. It's a large organization. There are very talented folks there, but of course, that's a cost. So in terms of providing a service, we have to go through that cost model. I hope that helps.

MR. BANDY: Jeff.

MR. STALNAKER: It's an interesting question and it's been asked of me many, many times. It seems like some of your features -- not all of our features -- remember I said 14 features? So we're not talking about a couple. But I've gotten the question that that ought to be something the phone company does and it ought to be part of my basic service. I should be able to control who can call me because I'm paying for the phone. You can use that for your mobile phone, too. That's why you should get PrivacyStar.

We do offer PrivacyStar -- I don't think I said the price point -- but we are lower than some of the operators, just as a side note. But it's free for seven days and then $2.99 per month. One of the things that we can do for operators is to be able to modify the features there. So if you just wanted call blocking and text blocking, complaint filing and maybe directory assistance, we can make that profile for you so that we know you are a Verizon customer and you only get these five features to really address some of the questions that we get along those lines.

MR. BANDY: This is a question for Andy. With the *57 call trace, if someone spoofed their number will you get additional information that might actually lead you back to the actual calling number -- in the case of a telemarketer -- who is spoofing?

MR. WHITT: Yes. As was said a couple of times today, when you think about the network, we had a comment earlier about ANI, Automatic Number Identification. If you pick up your phone and you dial 9-1-1, you want to make sure your number gets to the 9-1-1 service answering positions.

So in the network, especially in SS7, which was talked about a couple of times today, but in SS7, there's a lot of information that's passed when calls are set up. So when a person gets that abusive or threatening call, they do *57. The point there is that there is a record of many data points. It was just the previous presentation where someone talked about call records.

So we have some quite detailed call records that that particular record is captured so we don’t have to go hunt for it. It's formatted in such a way that our nuisance call center, the Unlawful Call Center, can grab that very quickly with the additional network signatures and information that our technical and support folks can then be evoked very quickly and take that data and be able to walk back through that network and at least see, ultimately, where it came into us from. And if it’s another carrier, then having to work with, in many cases, the subpoena process law enforcement to get the next carrier to give us that next piece because in most cases we're all capturing those records and that data is in place. So yeah, there's more.

Spoofing the number doesn't completely deter us, from the network perspective, getting back to that source.

MR. BANDY: Why are Go Phones legal? They're untraceable. Does anyone make the defense of disposable, prepaid mobile phones?

(No response.)

MR. BANDY: No?

MR. WHITT: Why are they legal?

MR. BANDY: I don't know if Verizon has a prepaid business.

MR. WHITT: Yes.

MR. BANDY: What would those guys say if they were up here today?

MR. WHITT: I wouldn't want to speak for them, but I think the answer is, to some extent, in my mind, you know, we have customers that we prequalify. So if somebody calls up and they want a service, you know, a wireless service, VoIP service or landline, there are all different service types. We do validations.

There are certain things that qualify that individual because if you're a post-pay customer, then there's an assumption that that bill will be paid one month later. So in some cases, for many reasons, maybe not even their fault, folks don’t have good credit and in some cases it can actually disqualify them from that agreement, for example, college kids. When I was paying for my children's cell phones, prepaid is a beautiful thing. You get 100 minutes and that's all you get.

So, again, I think the important thing is we're a market-driven, market-based industry and it serves a very good purpose. But can it be used for the bad guys? Yes. They show it in every thriller movie that's out there right now. They have phones that they run in and buy, program it, call and dump.

MR. BANDY: I would venture to say, and I am in no means an expert on it, that there is a segment of the population and a market for those products. Though I'm sure lots of people use those types of products for legitimate purposes and in a society where having global communications is so important, you want to make sure that those segments of the population certainly have access to those types of technologies.

I think the theme of today is that there have been technological innovations in our telecommunications. They've had some unwanted and undesirable side effects. I think mobile disposable phones falls into that.

This next question I think is more for me. Should people really register on the Do Not Call list? Doesn't that give telemarketers confirmed working numbers? Shouldn’t we assume really bad guys use the DNC list as a lead list? Has the DNC list outlived their usefulness?

Unless one of you guys want to take a crack at it, I'll take a crack at it. I think, yes, people should register on the DNC list. We focused a lot on robocalls and what bad guys are doing, but there are a lot of companies out there, legitimate marketing companies, that download that list and respect it and do not call consumers that have registered their numbers.

So people who do not register their numbers on the Do Not Call List, they could see an increase in legitimate telemarketing calls. If the goal is I don’t want to receive as many telemarketing calls, then you should've registered on the list. The second reason is if you do get illegal calls -- well, certain types of calls will only be illegal if you're registered on the list.

So if you get calls you don’t want and you file a complaint and it turns out you weren't registered on the list, then it inhibits our ability to pursue people that are engaged in illegal telemarketing and it really limits what can be done to sort of help address that problem.

One other point I want to make is as to the robocalls, you don’t have to be registered on the Do Not Call List. It is illegal to make a telemarketing robocall, regardless of whether you're on the list. I wanted to make sure that's clear. So you don't need to register for robocalls.

As for the point about can't the bad guys download the list and say well, I know maybe my legitimate competitors aren't calling these people because they're respecting the list, but that's an untapped market for me. I think that's a possibility, sure, but I think overall, in balance, the ability to stop the legitimate telemarketing greatly outweighs the fact that the bad guys may access the list. Plus, there's a fee. In the world of illegal telemarketing where margins are very, very thin, paying the fee to access the list just so you can call those people is probably less likely. So I think on balance, people are much better off by registering their numbers on the list. So that's my defense of the list.

Does anyone have any questions? I'm fresh out of cards and we have a little extra time.

(No response.)

All right. Well, thank you. Oh, we have one question.

MR. BELLOVIN: I'll give one answer on the prepaid stuff: foreign tourists.

MR. BANDY: Oh. Just for people on the internet and online, Steve Bellovin, our chief technology officer noted that prepaid mobile phones are very valuable to foreign tourists who use them, presumably for legitimate purposes and not to bombard locals with illegal telemarketing calls. Excellent point. Thank you. All right. Thank you to our panel.

(Applause.)

ANNOUNCEMENT

MS. DAFFAN: And now it is my great pleasure to introduce David Vladeck. He is the fearless, innovative leader of the FTC's Bureau of Consumer Protection, which makes him the perfect person to make this announcement.

MR. VLADECK: So this is the moment you've all been waiting for and I'm really gratified to see so many people still here.

I want to thank all of the panelists, the people here, the people who are watching on this on their web for sharing their perspectives today. This has been a terrific day. This has been the summit that we really needed. Robocalls are on the rise and we need to address this problem.

Here, at the FTC, one of our mottos is "Actions speak louder than words." And it is in this spirit that I am very proud to announce a first for the FTC, a formal challenge to innovators in the United States.

Here's the challenge: develop a technological solution that will reduce, substantially, the number of illegal robocalls consumers get, both on their landlines and on their mobile phones. Using challenge.gov, we are tapping into your create spirit, your technical expertise and your ability to innovate.

We are calling on you, college students, doctoral candidates, Ph.D.'s, all of the above to go out and to try to design a new system that will block illegal robocalls but let permissible robocalls through.

What do we want? We want a robocall blocking system that is practical and that works. We want one that is easy to deploy, easy to use. One that is practical and we can deploy quickly. We want one that will not place burdens on consumers. So technology is our goal. New technology is our goal.

What about existing solutions? Those people who are innovators who have already developed partial solutions, can they win the challenge? The answer is no. We're looking for new solutions. Unless you really revise existing ones and make them new, we're not interested.

Who does this cover and what are your incentives to do this? One incentive is for companies or organizations with fewer than 10 people, if they innovate and give us a design that works, the Federal Trade Commission will award $50,000 to an eligible winner. This is the first time the FTC has engaged in this kind of grant activity. We are joining other federal agencies that have used challenge.gov to promote needed innovation in a market that has not delivered the innovation that we need.

Next question. Who is going to evaluate our submission? Well, we have a panel of three experts. You met two of them this morning. First, there is our own Steve Bellovin, the FTC's chief technology officer. Next, there's Henning Schulzrinne, the FCC's chief technology officer, a colleague of Steve's at Columbia.

Last but not least, Steve and Henning will be joined by Kara Swisher of All Things Digital, or as some people know it as All Things D, an expert in consumer technology products and user experience.

How are we going to support your efforts other than dangling a fair amount of cash in front of you? Well, here's what is really important. For those people who are going to try to accept our challenge and design the next generation robocall blocker, here's what we're going to do. We're going to make available to you the FTC's complaint data on robocalls if you accept our challenge.

The complaints date back to June 2008 and will be updated and provided to you every two weeks. Of course, we will redact them to protect consumers’ privacy and personal information, but what we can release should be very helpful. It will be information about the phone number complained about, the business name reflected on caller ID; the consumer's area code, and the approximate time the calls were placed.

Now, you can and we would urge you to check challenge.gov for the specific rules, requirements, and frequently asked questions that will govern this challenge. So far, nearly 50 federal agencies have used this innovative approach to solve problems, and I am absolutely delighted that the FTC is joining that group. So this challenge officially opens on October 25th. This is sort of a sneak preview. The deadline for submissions will be January 17, 2013. So get to work now. We will announce our winners during the first week in April 2013. So we'll meet back here then.

So the FTC is attacking illegal robocalls on all fronts. One of the things that we can do as a government agency is to tap into the genius and technological expertise among the public. We think this will be an effective approach in the case of robocalls because the winner of our challenge becomes a national hero.

Now, think about it. The most important incentive of all is you will be a national hero.

Everyone in the United States wants to put Rachel and her robotic colleagues in our rearview mirror. If for no other reason, there is plenty of glory for the winner of this challenge grant.

Thank you again for being here. Thank you to our wonderful team from the Division of Marketing Practices, Bikram, Rob, Robocop Maxim, Kati Daffan, Lois Greisman and the wonderful people from the Division of Consumer and Business Education who did all these great graphics, and most importantly, designed our Rachel poster.

Thank you for a great day. There will be a press release announcing this challenge grant, posted on our website, probably right about now. So thank you all very much.

(Applause.)

(Whereupon, at 4:50 p.m., the Summit was concluded.)

* * * * *

CERTIFICATION OF REPORTER

MATTER NO.: P034412
MATTER NAME: DO NOT CALL ENFORCEMENT
HEARING DATE: OCTOBER 18, 2012

I HEREBY CERTIFY that the transcript contained herein is a full and accurate transcript of the notes taken by me at the hearing on the above cause before the FEDERAL TRADE COMMISSION to the best of my knowledge and belief.

DATED: OCTOBER 30, 2012

GERVEL WATTS

CERTIFICATION OF PROOFREADER

I HEREBY CERTIFY that I proofread the transcript for accuracy in spelling, hyphenation, punctuation and format.

SARA J. VANCE