Dialing Back:
How Phone Companies Can
End Unwanted Robocalls

Maureen Mahoney

November 2015

Table of Contents

ACKNOWLEDGMENTS

Dialing Back: How Phone Companies Can End Unwanted Robocalls

EXECUTIVE SUMMARY

The Do Not Call list, federal law enforcement efforts, and actions by the states have not been enough to protect Americans from the flood of unwanted robocalls that have become rampant in recent years. Hundreds of thousands of people complain each month to the Federal Trade Commission (FTC) about unwanted calls,[1] and it's estimated consumers lose $350 million a year to phone scams.[2] Thanks to rapid advances in Internet technology, robocallers can make thousands of auto-dialed calls per minute for a relatively low cost.[3] Robocall scammers easily escape detection and punishment by operating overseas[4] or using software to disguise—or spoof—their name and number.[5] The problem is so bad that federal agencies and Congress have been exploring solutions to the unwanted robocall problem.[6]

Technological solutions are necessary to address this problem. **A number of leading experts agree that phone companies have the power right now to implement technologies to dramatically reduce robocalls.**

Consumers Union surveyed a variety of experts and innovators and found there are at least four proposed and existing robocall filtering technologies that phone companies could pursue to help protect their customers from unwanted robocalls. One solution, the Primus Telemarketing Guard, has been successfully implemented for traditional and broadband phone lines in Canada,[7] which calls into question why similar technologies have not been offered in the United States.

Consumers Union launched a nationwide grassroots campaign in February 2015 to convince the major phone companies to offer customers free robocall blocking tools.[8] Over 500,000 Americans to date have signed the petition at EndRobocalls.org,[9] but the major phone companies have failed to provide their customers with meaningful relief. Right now, consumers with traditional analog landlines have only limited options to protect themselves from unwanted calls, such as obtaining inadequate blocking services from their phone company, or buying a phone or call blocking device that allows them to stop selected numbers.[10] And while many smartphone users and those with Internet-based phone service now have access to advanced third-party blocking tools,[11] the smartphone tools may work better if offered to consumers through the phone companies.[12] Moreover, the advanced blocking tools may be more widely used if provided directly by the carriers.

In June 2015 the Federal Communications Commission (FCC) made clear that phone companies have the legal authority to offer call blocking tools to their customers,[13] and FCC Chairman Tom Wheeler has urged them to do so.[14] But the top phone companies have resisted offering advanced filtering technology to all of their customers, citing concerns that customers may not receive wanted calls.[15]

Consumers Union interviewed a number of leading experts to find out what more phone companies could do to block unwanted calls. We found that phone companies could pursue at least four proposed or existing advanced filtering technologies that would provide customers substantial protection from unwanted robocalls.

- Phone companies could easily offer a filtering service directly to consumers with modern phone lines. For example, third-party companies have already developed smartphone apps that block unwanted calls. And Nomorobo, a free robocall blocking service, is currently available to many consumers with Internet-based service, or VoIP (Voice over Internet Protocol).

- Filtering tools could also be offered to consumers with traditional landlines. The Primus Telemarketing Guard has been available at no extra cost to traditional landline and VoIP users in Canada for years. And, according to Primus Canada, it could potentially work for traditional landline, VoIP, and wireless customers in the United States. Filters that can block calls at the "gateway" between networks have also been proposed and could potentially work for traditional landline, VoIP, and wireless customers.

- Companies have the technology to reduce call "spoofing"—the practice of disguising the origin of robocalls on Caller ID.[16] This would improve telephone security and call filtering techniques.

- Phone companies' current robocall blocking offerings are insufficient and often costly for customers.

- Filtering unwanted robocalls would also benefit phone companies by reducing customer complaints and ultimately lowering customer turnover.

Recommendations:

- Phone companies should immediately offer free robocall-filtering services to all of their customers based on latest available technology.

- Phone companies should immediately develop "Do Not Originate" techniques to reduce spoofing by fraudulent callers.[17]

- Phone companies should continue to pursue call authentication strategies as a long-term solution to the spoofing problem.

WHY AMERICANS ARE DELUGED WITH ROBOCALLS

- 217.9 million phone numbers are registered on the Do Not Call list;[18]
- 305,000 complaints about Do Not Call violations were made in September 2014;[19]
- The FTC has recovered less than 9 percent of the $1.2 billion in fines levied for "DNC [Do Not Call] & Robocall" violations.[20]

The Do Not Call List Has Not Stopped Robocalls

Federal regulatory efforts haven't been enough to stop unwanted robocalls. In part because of changing technology, the numbers of unwanted robocalls have soared,[21] and it has become much harder for scammers to be held accountable. Many of the unwanted calls come from overseas robocallers who don't respect the Do Not Call list and don't fear getting caught.[22] Moreover, because the registry is designed to protect consumers from unwanted telemarketing calls,[23] consumers may receive legal, but unwanted, robocalls at home from politicians or other groups.[24]

Millions of Americans have placed their phone numbers on the Do Not Call Registry since it was established in 2003 in the hopes that it would stop unwanted calls.[25] There are now nearly 218 million phone numbers on the registry.[26] The rules make it illegal for most commercial telemarketers to contact numbers on the list without permission,[27] whether it is an auto-dialed or a manually-dialed call.[28]

Still, many types of calls are exempt from the Do Not Call list and other federal rules, so consumers continue to get legal calls they don't want. Live telemarketers[29] can autodial home phones[30] for up to 18 months after the last time the consumer did business with that company.[31] And non-profits, pollsters and politicians are permitted to autodial home phones[32] on the DNC list without first getting permission.[33]

Recently, the FCC expanded the types of acceptable auto-dialed calls to cell phones. Now, businesses may send a limited number[34] of informational robocalls to a cell phone for financial reasons such as fraud, a data breach,[35] or pending money transfers.[36] Healthcare providers may also send a limited number of robocalls to cell phones for appointment reminders, prescription refills, pre- and post-care instructions, and billing.[37]

Enforcement Is Challenging

Why is enforcement so difficult?

- Scammers hide their identities by placing "spoofed" calls through Internet-based networks (VoIP);
- Calls placed over VoIP often must be traced through multiple carriers, making it time-consuming to track down scammers;
- Many scammers are located overseas, where they are difficult to catch;
- Scammers try to spend their money as quickly as they get it, so it can be difficult to recover.

Technological innovations have unleashed powerful economic incentives for scammers to robocall consumers. New technology allows robocallers to make thousands of inexpensive auto-dialed calls per minute.[38] For example, cloud hosting services and call-generation software

platforms let telemarketers send calls without purchasing costly hardware.[39] All they need is a disposable cell phone[40] or an account with a service that allows them to send these calls.

Others may set up fraudulent boiler rooms where live agents autodial consumers. Many of these boiler rooms are located overseas where they are off-limits to detection and prosecution.[41] The FTC doesn't have the authority to force an overseas carrier to turn over their call records to track down a scammer.[42] The Voice over Internet Protocol (VoIP) calls placed from overseas cost the same as a call made from the United States, so there is no financial incentive for scammers to set up shop in the U.S. where they can be more easily caught.[43]

Another technology makes it harder to track down where robocalls originate. Call "spoofing" disguises the caller's name or number on Caller ID, and can be accomplished through the use of an app.[44] While calls made on traditional landline phones correlate to a phone number tied to a physical location,[45] scammers using VoIP technology can use applications so that it appears they are calling from a different number. According to Vijay Balasubramaniyan of Pindrop Security, a company that combats phone fraud for businesses: "You can use [a VoIP] app and you can pretend to be anyone."[46]

There's little chance scammers using VoIP will be caught, because it is extremely difficult to track down the caller.[47] Calls placed over VoIP may be routed through several different carriers before they reach the consumer.[48] According to the FTC's Bikram Bandy, "It's not uncommon to see that these calls are routed through four, five, six networks."[49] But, Bandy notes that the FTC can often identify scammers by tracing credit card or debit card payments made by defrauded consumers.[50] A variety of factors further inhibit law enforcement efforts. According to the FTC, even if they find the scammers, they typically can recover only a small portion, if any, of the money taken from consumers. The scammers try to spend the money as quickly as they can.[51] "Enforcement has problems in terms of scaling, the time it takes to get one of these guys," said Henning Schulzrinne, Levi Professor of Computer Science and Electrical Engineering at Columbia University, and formerly the Chief Technology Officer of the FCC. Before the authorities could track them down, "they would disappear."[52]

Consumers Pay the Price

- Estimated $350 million lost by Americans to phone scams annually;
- $19 million lost to the IRS scam alone.[53]

> "A few months ago I received a call from a 'private caller.' That's how my doctor shows up, so I answered it. The caller said they were sending out new Medicare cards and wanted to verify my information. She verified my name, address, etc. Then she said get out your checkbook and read me the numbers on the bottom of the check. I knew this was my bank account number so I said I don't have a checking account. She angrily replied, you do too, it's with [a major bank]. Then I knew she already had too much info about me and hung up."[54] -- Gerald, Joshua, TX

Consumers are stuck paying the price for relentless robocalls, many of which are scams designed to trick them out of their money. Americans lose an estimated $350 million a year to phone scams. For example, consumers tell us that they frequently hear from the infamous "Rachel from Cardholder Services," a fraudulent robocall that promises to lower credit card interest rates for a lump sum.[55] Consumers also report receiving robocalls from crooks trying to charge them to activate "free" medical devices that a friend or family member has supposedly purchased.[56]

These calls are not only annoying, they can be downright threatening. In recent years consumers have received calls from scammers claiming to be Internal Revenue Service (IRS) agents, demanding money to cover a fictional tax bill.[57] Some consumers report being robocalled by debt collectors over money that they don't owe.[58] And crooks masquerading as tech support representatives try to fool consumers into paying them to fix a phony computer problem, or to allow them to install software that will extract their personal information.[59]

Spoofing makes scamming consumers out of their money even easier, since they are more likely to pick up a call if they are tricked into believing it is legitimate. For example, IRS scammers often spoof a Washington, D.C., area code, where the tax collection agency is based.[60] Or scammers might spoof a consumer's own phone number.[61] Their tricks may be effective in part because people tend to have more faith in their Caller ID than, for example, an email address. Research Scientist Payas Gupta of New York University Abu Dhabi et al. argue, "[A]ttacks that utilize the telephone as a resource are more successful because people in the past have trusted the telephony channel."[62]

Scammers have plenty of incentives to robocall consumers. Not only can they steal money from the consumer, but they can sell credit card and other personal information they obtain from victims to other criminals looking for new targets.[63] One scam victim can end up being victimized multiple times.

PHONE COMPANIES CAN DRAMATICALLY REDUCE ROBOCALLS

> "There are at least eight technical solutions that, individually and in combination, can reduce robocalls."[64] –Prof. Henning Schulzrinne, former Chief Technology Officer of the FCC

Experts argue that phone companies have the power right now to implement new technologies to dramatically reduce robocalls. They have proposed or created at least four types of advanced robocall-blockers that can stop unwanted calls with little intervention on the part of consumers. One of these proposed solutions, the third-party filters that operate through "gateway" technology, could potentially work for customers who use traditional landlines as well as those who use cell phones or Voice over Internet Protocol (VoIP),[65] according to Henning Schulzrinne. Another, the Primus Telemarketing Guard, has been offered to broadband and traditional landline consumers in Canada for several years.[66] These tools could sort through calls to stop unwanted robocalls so that consumers don't have to manually block calls one by one.

Phone companies also have the tools to immediately reduce call spoofing. Carriers could pursue Henning Schulzrinne's conception of a "Do Not Originate"[67] list that would protect callers from some of the most commonly-spoofed numbers, like the IRS. Placing a number on the Do Not Originate list would tell companies to block calls with that number originating from certain providers or gateways. In the next few years, carriers also should implement call authentication strategies so that callers' identities could be confirmed when placing calls,[68] and consumers might once again trust their Caller ID.

Four Robocall Filtering Technologies

<u>Nomorobo</u>

This filter works by blocking "blacklisted" numbers—phone numbers reported to the FTC for Do Not Call list violations, and numbers that consumers report are used by robocallers.[69]

Nomorobo works through a service called "simultaneous ring" that is free to most VoIP users and lets a phone call ring in two locations at once. Currently, Nomorobo is only available to consumers with VoIP service.[70] Customers can have a phone call ring on both their home and cell phone at the same time. Subscribers arrange for incoming calls to reach their own number and Nomorobo servers simultaneously. When Nomorobo identifies an unwanted call, it zaps the call after the first ring.[71]

Additionally, Nomorobo tries to identify calls that are highly likely to be spam by using a recently developed system known as a "honeypot."[72] Honeypot software collects information about calls placed to a pre-designated group of phone numbers[73]—in this case, numbers that had been abandoned by consumers for too many unsolicited calls. Since legitimate callers are probably not calling an inactive number,[74] Nomorobo is able to blacklist numbers harvested from the honeypot.

According to Payas Gupta, Research Scientist at New York University Abu Dhabi, "telephone honeypots are promising" in reducing robocalls and recommends the phone companies and security vendors use them. He explains, "When a call comes in, then one can provide a variety of responses ranging from picking up the call, automated interaction with the caller, monitor the calling patterns, recording the calls if legally allowed, etc." further noting that "if the number is spoofed, one can try to identify the source location by analyzing audio and calling patterns." Moreover, if used by carriers, honeypots could be even more effective in identifying unwanted robocalls. Says Gupta, "Telcos could share information from the telephone honeypots and mark unwanted calls in real time."[75]

Ultimately, Nomorobo runs all the collected data through an algorithm to identify suspicious calls.[76] In this way, Nomorobo can even block "spoofed" calls. Company owner Aaron Foss explains: "A robocaller might spoof a random number but when that fake number starts calling 5,000 people in an hour, well, humans don't call like that."[77] Callers identified by the algorithm as suspicious are asked to input a number to prove they are not machines.[78] To ensure legitimate robocalls like school closings and emergency notifications get through, they are placed on a whitelist at the request of consumers.[79]

About 280,000 consumers have subscribed to Nomorobo,[80] and many have reported positive results. Michael from Tampa is one of the most enthusiastic. He reports that: "Since adding the Nomorobo service, my phone has gone from ringing up to 20 times each day with useless calls, down to allowing just the one or two calls each day that I really want to receive. The silence in my home is gratifying, and Nomorobo does not seem to mistakenly block any calls that I want to receive."[81] Twenty-five of a group of forty volunteer testers for Consumer Reports gave the service the highest rating on a scale of one to five, and an additional nine volunteers gave it four or four and a half stars.[82]

Primus Telemarketing Guard

Primus Canada, an independent Internet and phone provider that provides services to hundreds of thousands of Canadian customers, developed Telemarketing Guard, another filtering system that tackles the problem of unwanted robocalls. It's been available for free to Primus's traditional landline and broadband customers in Canada since 2007.[83]

The system harnesses user feedback and its monitoring system to identify suspicious calling patterns and screen unwanted calls before the customer's phone rings. Customers using Telemarketing Guard can also control their own blacklists and whitelists via an online portal. If a call is suspicious but isn't on the blacklist, then it is "greylisted," and the consumer is able to decide whether or not to take the call, block it, or send it to voicemail.[84]

When a greylisted call comes in—those numbers that have been identified by other customers as possible spam—the caller is asked to identify themselves to the recipient. They are invited to press 1 and then record their name. The recording is played to the consumer, who can decide to send it to voicemail, answer it, or hang up.[85]

According to Brad Fisher, Senior Vice President of Marketing and Product at Primus Canada, consumers receive at least 20 fewer telemarketing calls per month with the service.[86] The service also helps customer retention for the phone company. It has been reported that 87 percent of customers cite the Telemarketing Guard as the main reason they continue to use Primus Canada.[87]

It's rare that people making legitimate calls complain about getting intercepted by the Telemarketing Guard, according to Fisher: "A caller can only be blocked if they are on the customer's personal blacklist." He elaborates, "If a call is wrongly intercepted by the greylist, the customer can accept the call and easily add that caller to their personal whitelist."[88]

Though Primus Canada says that its software is highly adaptable to US networks, phone companies here do not offer it.[89] While a few companies expressed interest in the service after Primus presented at a FTC Robocalls conference in 2012, they ultimately did not pursue it.[90] USTelecom speculated that the "legal impediment"—their concern that the software would violate carrier obligations to avoid blocking calls—accounted for the lack of interest.[91] But the FCC ruled in June 2015 that phone companies can legally use this type of software to block robocalls.[92]

Third-Party Filters for Gateway Technology

Companies could work with a third-party service to filter unwanted robocalls for consumers. Schulzrinne notes that these filters could be extended to all customers by re-programming the software on the computers that serve as a "gateway" between VoIP lines and the legacy systems that deliver the calls to the consumers.[93] While these tools have not yet been brought to market, as conceptualized, they could block or direct certain types of calls to voicemail, or to another party based on information reported to carriers by consumers.[94] Schulzrinne says, "They could start essentially making it possible for third parties to do filtering in a robust way."[95] Phone companies could use third-party filters to screen unwanted robocalls on landline, broadband, and cell phones.[96]

It's clear that phone companies could do more to work with third parties to address robocalls. When discussing the role of gateway providers in stopping unwanted calls, Adam Panagia of

AT&T[97] noted that "We're really not there yet on sharing originating numbers that are involved in robocalling campaigns . . . I think that's somewhere we need to be and . . . the third-party blocking applications . . . already have a lot of these numbers that are available. . . .[W]e need to do a better job in sharing that intelligence across the industry."[98]

Smartphone Apps

Consumers can currently download a number of smartphone apps to block robocalls to their smartphones.[99] But carriers could also offer that technology to customers directly. For example, the Call Control app (14 day free trial, then $2.99 per month) builds its blacklist from information collected about spam calls from its 10 million users. They also block numbers identified as spam by the Indiana Attorney General's office and the federal Do Not Call list. Finally, they use algorithms to monitor call activity across their Call Control users to identify bad robocallers. For example, Ben Sharpe of Call Control says, "We can tell if a telephone number of a large bank has been hijacked and is being spoofed."[100]

PrivacyStar is another app that can automatically block calls they've identified as fraudulent. It blocks spam calls, and has a green, yellow and red color-coded system for incoming calls to indicate to the user whether the call is likely legitimate. The app also allows consumers to easily report call violations to the FTC. To access all of the features of the service, consumers may be charged a fee.[101] Jonathan Sasse of PrivacyStar says that if the scammer is "spoofing a number like your own, we can block those. If they're spoofing a number that's otherwise inactive, or if it belongs to a real business, we see abnormal activity, that's an opportunity to blacklist."[102]

Schulzrinne points out that some of the apps don't work as well as consumers would like and have mixed ratings online.[103] He notes that "Current platforms aren't really designed to make it easy for third parties to inject themselves into the phone stream."[104] But, he says, "With the cooperation of carriers, [they] could work better than they do today."[105]

Phone Companies Can Implement Robocall Filters

Phone companies could offer filters to protect consumers from unwanted robocalls. According to Schulzrinne, the third-party filters installed at network "gateways" potentially could be offered to consumers with landline, VoIP, and wireless phones,[106] while Primus Canada argues that Telemarketing Guard potentially could be offered to these three types of services in the United States. Offering the technology associated with the smartphone apps to traditional landlines would likely be more cost-intensive and would differ for each phone company.[107]

Primus Canada's Telemarketing Guard potentially could be used for landline, VoIP, and wireless phones in the United States, according to the company.[108] "Telemarketing Guard does not require customers to purchase or install any equipment or software, or any additional features," says Brad Fisher. Further, he notes that "The system works at the network level, through very typical equipment."[109]

A software upgrade also would allow third-party gateway filters to work with major U.S. phone companies, says Schulzrinne. These gateway filters have been conceptualized but not yet developed.[110] Schulzrinne explains that they could be added as part of a software upgrade to the modern gateways between the Internet-based lines through which robocallers send calls, and the lines that actually deliver the call to the consumer. He says that interfaces at the gateway could be configured to screen unwanted robocalls. The gateways are "designed to be highly programmable," and they feature interfaces to counter fraud.[111] According to Schulzrinne,

adding new interfaces to these gateways to filter robocalls would not be very different from steps the phone companies already take to address fraud.[112] When asked about the cost, he said that it is "well within the realm of feasibility."[113]

App makers have reached out to phone companies about applying the technology. Says Jonathan Sasse of PrivacyStar, "We've been trying to work with the carriers to improve the situation if not stop it," citing Sprint Prepaid, Boost, MetroPCS, Virgin Mobile, and TracFone as companies for whom they have offered products for Android phones.[114] According to Sasse, "We collaborate with the carrier on pricing, features and distribution."[115] A spokesman for TracFone, Evan Oei, says PrivacyStar's Call Detector app is available to customers through the Google Play store.[116]

Ben Sharpe says that Call Control has discussed with carriers the option of applying the technology that powers their smartphone app to the carriers' systems to filter robocalls for all landline, mobile and broadband consumers. According to Sharpe, the cost to integrate the technology would depend on the carriers' existing set up.[117]

As for the prospect of applying similar technology to traditional landlines, Jonathan Sasse of PrivacyStar envisions that consumers could go online to manage their account and stop different types of calls, though he admits it would "require upgraded technology."[118] He said the required upgrade "isn't trivial," but depends on the carrier and the systems they have in place.[119] Similarly, Sharpe says that they have been offering technology "to the phone companies for the last three or four years, and predicts options could be made available for customers to "access their personal settings on their phone or web portal for their landline" and set up do not disturb mode, personal whitelists and blacklists, as well as block private and unknown calls.[120]

Nomorobo founder Aaron Foss has made his service available to VoIP customers that have enabled the simultaneous ring service, even without their phone company's cooperation.[121] Foss says his program theoretically could be used by all phone customers, saying carriers need only switch on simultaneous ring for landline and wireless. According to Foss, this could be handled through "software switches"—meaning the software that connects the lines through which the call originated and those that actually deliver the call to the consumer.[122] Yet he admits that phone companies may be reluctant or unwilling to make this upgrade because traditional landline networks are old and unreliable.[123] As for the prospect of extending simultaneous ring to traditional landlines, Schulzrinne notes that "Older landline systems may not support simultaneous ringing or carriers may choose not to enable the feature."[124] For its part, USTelecom points out that phone companies are in the process of transitioning to Internet-based networks, and "Even where it might be possible to deploy simultaneous ring within an existing TDM network, it is not clear whether it could be accomplished while still being able to offer a NoMoRobo-type solution on a cost effective basis to end users."[125]

Phone Companies Should Use Anti-Spoofing Techniques

To ensure effective robocall blocking, the phone companies also must use technology to identify spoofed calls. The filtering tools described above could be even more effective if the phone companies' Caller ID could be trusted. Carriers should work to address spoofing to establish telephone security. There are currently at least two promising options to do so.

"Do Not Originate" to Reduce Spoofing

Phone companies could cut back on spoofing by developing a "Do Not Originate" list. As described by Henning Schulzrinne, some carriers and third-party companies operate gateways between the calls placed over VoIP and the traditional phone lines that deliver the calls to the consumer. Commonly spoofed organizations, such as banks, law enforcement, or the IRS, could place themselves on a list and notify the gateway keepers that calls featuring their numbers that originate from certain gateways or providers are likely fraudulent and should be stopped.[126] This technology would stop only the spoofed calls from numbers placed on the "Do Not Originate" list.[127] Carriers already have the technology to implement such a system.[128] Adam Panagia of AT&T says of this proposal,[129] "In most cases I think that would be very helpful,"[130] though cautions that it could inadvertently disrupt some legitimate calls.[131]

Call Authentication to Address Spoofing

A group within the Internet Engineering Task Force (IETF), an open, standards-making organization,[132] has been working to develop Internet standards so that callers and carriers can confirm that they are the owner of a particular phone number.[133] A second, but related group in the IETF is working on verifying the names that appear on Caller ID.[134] This would address the problem of call spoofing that is so common with the spread of VoIP.[135] While these standards would only apply to calls placed with VoIP technology, they would benefit consumers using all types of phone lines because most fraudulent robocall attacks originate from VoIP.[136] AT&T and Verizon have said that they are working with the IETF on these proposals.[137]

Unfortunately, this process could take years and a great deal of coordination among countries to implement—according to one recent estimate, five to seven years.[138] Schulzrinne notes that these standards would require software upgrades.[139] Moreover, the standards are voluntary, not mandatory so carriers would not be required to adopt them.[140]

Nevertheless, this is a promising long-term solution to the illegal spoofing problem. Carriers should continue to encourage the development of these standards and to implement them when completed.

PHONE COMPANIES' CURRENT CALL BLOCKING OFFERINGS FALL SHORT

Few Services for Traditional Landline Customers, More for VoIP

Unfortunately, top U.S. phone companies do not offer their traditional landline customers — approximately 50% of home phone users[141]—the type of advanced call-blockers described above, and only limited options for those who want to block robocalls. For example, AT&T, Verizon, and CenturyLink allow traditional landline customers to block just a small set of numbers that they identify themselves, as well as anonymous calls. Not only is inputting selected numbers a hassle, but it's not always free.[142]

Consumers tell us that only being able to block a few numbers makes these tools ineffective against spoofers. Steve of Altadena, Calif., says, "I add a number to block a call and I never hear from that one again. That's because telemarketers use zillions of numbers, so blocking any one of them is pointless. It's like playing whack-a-mole."[143]

Likewise, phone companies typically offer Anonymous Call Block and Call Trace. Costs vary for these services, but traditional landline customers can pay $6 a month for Anonymous Call Block.[144] Call Trace is usually charged on a per-use basis, but can cost up to $10.[145] These tools can be useful in certain circumstances, but they fail to effectively and proactively block many robocalls.

CenturyLink also offers a service called No Solicitation. It works by playing a recorded message explaining that the customer does not accept unsolicited telemarketing calls. It invites the caller to press one, or remain on the line.[146] However, the service does not disconnect the call if the caller does not press one, so consumers may still receive unwanted robocalls.[147]

Consumers who subscribe to VoIP phone service have more powerful call blocking options, typically for no extra charge. For example, many VoIP subscribers, including AT&T U-verse and Verizon FiOS customers, can sign up for Nomorobo, since it is enabled to work with any "simultaneous ring" service.[148] Other options include AT&T U-verse's "Call Screening" product, which allows consumers to "whitelist" up to 20 numbers and block the rest.[149] Verizon FiOS customers can block up to 100 numbers,[150] and the VoIP provider VOIPO has a service called Telemarketer Block, which directs calls identified as telemarketers to voicemail.[151] VOIPO also formed a partnership with Nomorobo to offer the service to its customers.[152]

Still, options are limited for traditional landline customers, and the transition to fully IP based networks could take several years.[153] Consumers may buy devices to plug into their landline and VoIP phones to block unwanted calls. Some devices let consumers build blacklists of unwanted numbers, while others allow them to block all calls except for a select number of "whitelisted" numbers. Some work both ways. These devices typically cost between $50 and $110. Many consumers who tested these devices for Consumer Reports reported that they liked the protection offered by the call blockers.[154] Some phones, for home use[155] and wireless,[156] allow the consumer to enter or select numbers they would like to block. While these products may offer much-needed robocall blocking to consumers, they typically put the responsibility on consumers to enter the numbers to block or allow. Moreover, the stand-alone call blocking devices are not free.

See the Appendix for more details on the limited call blocking options currently offered by major phone carriers.

Major Phone Companies Have Resisted Advanced Call Blocking Tools

> "Phone companies, please start letting your customers request to have robocalls blocked."[157] --FCC Chairman Tom Wheeler

AT&T, Verizon, and Century Link tell Consumers Union that they are doing everything they can to stop unwanted calls. But the phone industry, despite pressure from lawmakers and regulators, has resisted offering new, comprehensive options to all consumers to stop robocalls.

On June 18, 2015, the FCC voted to make it clear that phone companies can give their customers the choice to use call blocking technologies. FCC Commissioner Mignon Clyburn called the decision a "win" and said that call blocking tools are "exactly the type of offering that we want to encourage carriers to provide."[158]

State attorneys general welcomed the FCC's decision, and recently called on the carriers to offer better tools to their customers. In July 2015, forty-five attorneys general sent a letter to

AT&T, Verizon, CenturyLink, Sprint, and T-Mobile, and urged them to provide the latest call blocking technology to their customers.[159] Federal lawmakers have also spoken out on the issue. In August 2015, eight US senators instructed the FCC and the phone companies to work together to create and offer advanced call blocking tools to consumers.[160]

The telecom industry has so far resisted the pressure from lawmakers. The CTIA, which represents the wireless companies, shrugged off responsibility for the robocall problem. In July 2015 they said: "[T]he attention to stop [robocalls] needs to focus on those bad actors who are willfully and blatantly ignoring the laws."[161] USTelecom responded to the FCC vote by reiterating their commitment to stopping robocalls, but protested that: "[T]here is no single technological solution to solving this problem[.]"[162]

As part of the End Robocalls campaign, Consumers Union sent letters to AT&T, Verizon, and CenturyLink, asking them to provide customers free robocall blocking tools.[163] The companies responded that they were doing their best to stop robocalls, and that consumers could take advantage of the offerings already available to them.[164] Verizon has suggested that "Educating consumers about robocalls would go a long way toward ensuring that [consumers] are aware of the various options available to guard against unwanted calls."[165]

Phone companies' responses to the letter from the attorneys general haven't been much stronger. Both AT&T and CenturyLink have said that customers should use their existing call blocking options,[166] but they offer only limited protection against unwanted calls. For its part, Verizon raised concerns that advanced robocall blocking technology might block legitimate calls, like emergency notices.[167]

While Verizon's concerns are understandable, tools like Primus Canada's Telemarketing Guard take steps to avoid blocking wanted robocalls. For example, the Telemarketing Guard relies on customer feedback to "greylist" calls. It's unlikely that consumers will flag emergency robocalls as unwanted. And, Primus Canada's experience is that legitimate callers have rarely been intercepted.[168] Finally, while no robocall blocking technology will be perfect, consumers should have the right to decide whether the benefits of any technology will outweigh any potential downside. Consumers can be informed of any risks associated with the tools in the form of a disclosure.

Ending Robocalls Will Benefit Phone Companies, Consumers

> "Being able to trust the traffic that enters their networks would be a good thing for [carriers]."[169] – Mustaque Ahamad, Professor, Georgia Institute of Technology College of Computing, and Co-Founder of Pindrop Security

It's in the best interest of the phone companies to immediately offer to customers the latest and best technologies to end robocalls. As Primus Canada's experience has shown, offering effective call blocking tools can reduce customer turnover. It could also reduce the amount of time spent dealing with problems consumers experience with robocalls. "The feedback from telephone companies is that problems consumers experience with robocalls are the number one customer complaint," says Ben Sharpe of Call Control.[170]

"This is a high value feature for our customers," says Brad Fisher of the Telemarketing Guard.[171] The VoIP provider VOIPO has even announced a partnership with Nomorobo to reduce calls, showing that call blocking could be used as a selling point.[172]

Also, ending spoofing would be beneficial for phone companies, because there's value in being able to identify and deliver legitimate calls to their customers, says Professor Ahamad.[173] Jonathan Sasse of PrivacyStar points out that carriers "don't want their networks to be polluted from these calls."[174]

Carriers also spend a lot of money in fielding customer complaints about robocalls. Eric Burger, Professor of Computer Science at Georgetown University, notes that handling customer complaints is quite expensive—and illegal robocalls are the source of many of these complaints. He notes that the money phone companies make from completing calls is outweighed by how much it costs to deal with customer service calls, as it costs "dollars per minute" to address consumers' concerns.[175]

Carriers should heed some of the lessons learned from the fight against email spam in the early 2000s, experts say. Consumers were overwhelmed with unwanted spam, but spam filters were able to direct scammers and unsolicited messages to separate folders. Balasubramaniyan of Pindrop Security says, "[T]hat's exactly the way the security in the phone channel is also going to go."[176]

RECOMMENDATIONS

- Phone companies should immediately offer free robocall filtering services to all customers based on the latest technology.

- Phone companies should immediately develop "Do Not Originate" techniques to reduce call spoofing.

- Phone companies should continue to pursue call authentication strategies as a long-term solution to the spoofing problem.

APPENDIX: PHONE COMPANIES' CURRENT CALL BLOCKING OPTIONS

This chart outlines the call blocking services available to customers of AT&T, Verizon, and CenturyLink in July-October 2015, based on areas in California, Washington State, and Pennsylvania, as well as general estimates. Where possible, information about the cost of the service was obtained online or through an online chat with a customer service representative. Customer service representatives provided additional information over the phone. Pricing and availability is subject to change and may differ depending on the area and calling plan. This is intended for reference purposes only. Please check with your phone company for the most current and up-to-date prices.

AT&T				
Service	**Description**	**Landline**	**U-verse (VoIP)**	**Wireless**
Call Block	Block unwanted numbers[177]	Block 10 individual and all anonymous numbers, $8.50 per month[178]	Block 20 numbers,[179] free[180]	Block 30 numbers, $4.99 per month[181]
Call Screening	"Whitelist" certain numbers, block the rest[182]	n/a[183]	Block all but 20 selected numbers,[184] free[185]	n/a[186]
Privacy Manager	Callers with suppressed Caller ID can be connected after providing their name[187]	Free[188]	n/a[189]	n/a[190]
Anonymous Call Rejection	Block numbers with suppressed Caller ID[191]	$8.50 per month, included with Call Block at no extra charge[192]	Free[193]	n/a[194]
Do Not Disturb	Stops all calls when enabled[195]	n/a[196]	Free[197]	n/a[198]
Call Trace	Dial *57 to report an obscene call to the police. Caller must then pursue issue with authorities[199]	Estimate of $4 per call[200] Free for unsuccessful attempts, charges vary for successful ones. Not for telemarketing calls[201]	$8.00 per trace[202]	n/a[203]

VERIZON				
Service	**Description**	**Landline**	**FiOS (VoIP)**	**Wireless**
Call Block	Block unwanted numbers	Block 6 or 12 numbers,[204] depending on area,[205] $6 per month[206]	Block 100 numbers,[207] free[208]	Block 5 numbers for 90 days for free. Block 20 permanently for $5 per month.[209] Anonymous calls blocked as well under the $5 plan.[210]
Anonymous Call Rejection	Block calls with suppressed Caller ID	Approximately $6 per month[211]	Free[212]	Can block anonymous calls through Call Block service.[213]
Call Trace	Can report calls to Verizon, "stored for future action"[214]	$10 per use[215]	Free[216]	n/a[217]
Do Not Disturb	When enabled, callers get recorded message or go to voicemail[218]	$6.10, but n/a to new customers[219]	Can select 10 callers to be allowed through. Free[220]	n/a[221]

CENTURYLINK			
Service	**Description**	**Basic Phone (Local only)**[222]	**Home Phone Plus**
Call Rejection	Block unwanted numbers[223]	Block 12-15 numbers,[224] $6 per month, with one-time $7 fee.[225] Block up to 25 through "Enhanced Call Rejection,"[226] $6 per month with one-time $7 fee[227]	Free (customers can choose 10 services for no additional cost)[228]
Anonymous Call Rejection	Block numbers w/out Caller ID info[229]	$6 per month[230]	Free
Call Trace	Can report disturbing calls. After three traces, can request further action from CenturyLink[231]	Up to $10 (if successful)[232]	Free [233]
Do Not Disturb	Stop incoming calls[234]	$3.95/month, one-time fee of $7[235]	Free
Caller ID with Privacy+, Security Screen	Privacy+ screens calls with suppressed Caller ID. They can be put through after the caller provides a name. With Security Screen, callers can be connected after providing their number.[236] Up to 25 numbers[237]	Privacy+: one-time fee of $7[238] Security Screen: $2.95 per month[239]	Free
No Solicitation	Callers hear a recording that asks telemarketers to hang up. Others are instructed to press 1 to continue, or stay on the line.[240]	$6.95 per month[241]	Free

NOTES

[1] Federal Trade Commission, *National Do Not Call Registry Data Book FY 2014* (Washington, DC: November 2014), 5, https://www.ftc.gov/system/files/documents/reports/national-do-not-call-registry-data-book-fiscal-year-2014/dncdatabookfy2014.pdf.

[2] Federal Trade Commission, Staff Report of the Bureau of Economics, *Consumer Fraud in the United States, 2011: The Third FTC Survey,* by Keith B. Anderson (Washington, DC: April 2013), https://www.ftc.gov/sites/default/files/documents/reports/consumer-fraud-united-states-2011-third-ftc-survey/130419fraudsurvey_0.pdf. There were an estimated 3.5 million telemarketing fraud cases in 2011 (p. 38). The median loss per case was $100 (p. 39). Therefore, an estimated $350 million was lost to telemarketing fraud in 2011.

[3] Andrea Rock, "FCC on How to Eliminate Annoying Robocalls: FCC Rules Are Designed to Protect Consumers, But the Onslaught Continues," *Consumer Reports*, January 14, 2014, http://www.consumerreports.org/cro/news/2014/01/how-to-eliminate-annoying-robocalls/index.htm.

[4] *Ringing off the Hook: Examining the Proliferation of Unwanted Calls, Before the United States Senate Special Comm. on Aging,* 114th Cong. (2015) (testimony of the Federal Trade Commission), 12, http://www.aging.senate.gov/imo/media/doc/FTC_Greisman_6_10_15.pdf.

[5] Ibid., 11.

[6] See, for example, Federal Trade Commission, "Robocalls: All the Rage, An FTC Summit," October 18, 2012, https://www.ftc.gov/sites/default/files/documents/public_events/robocalls-all-rage-ftc-summit/robocallsummittranscript.pdf; *Ringing off the Hook: Examining the Proliferation of Unwanted Calls, Before the United States Senate Special Comm. on Aging,* 114th Cong. (2015), http://www.aging.senate.gov/hearings/ringing-off-the-hook_examining-the-proliferation-of-unwanted-calls; Federal Communications Commission, "Workshop to Focus on Robocall Blocking and Caller ID Spoofing," September 16, 2015, https://www.fcc.gov/events/workshop-focus-robocall-blocking-and-caller-id-spoofing.

[7] Federal Trade Commission, "Robocalls: All the Rage," 219.

[8] Tim Marvin, "No More Complaining. Let's End Robocalls!" *Campaign Updates* (blog), February 17, 2015, http://consumersunion.org/campaign-updates/no-more-complaining-lets-end-robocalls/.

[9] Consumers Union, "End Robocalls," accessed September 18, 2015, EndRobocalls.org.

[10] "Robocall Blocker Review: Is There Any Way to Eliminate Those Maddening Calls?" *Consumer Reports*, last modified August 14, 2015, http://www.consumerreports.org/cro/magazine/2015/07/robocall-blocker-review/index.htm on call blocking devices; "Cordless Phones with Call Block," SmithGear, accessed September 1, 2015, http://www.smithgear.com/block-phone-calls.html for examples of phones that can block calls.

[11] CTIA: The Wireless Association, "Blocking Robocalls," *Your Wireless Life* (blog), accessed September 4, 2015, http://www.ctia.org/your-wireless-life/consumer-tips/blocking-robocalls. See also "Supported Carriers," Nomorobo, accessed September 21, 2015, https://www.nomorobo.com/signup. Many consumers with Voice over Internet Protocol (VoIP) service can obtain Nomorobo.

[12] *Ringing off the Hook*, (comments of Henning Schulzrinne, approximately 59:38).

[13] Federal Communications Commission, *Declaratory Ruling and Order*, CG Docket No. 02-278, WC Docket No. 07-135 (2015), 73, https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-72A1.doc.

[14] Tom Wheeler, "Another Win for Consumers," *Official FCC Blog,* May 27, 2015, https://www.fcc.gov/blog/another-win-consumers.

[15] Timothy P. McKone (Executive Vice President, Federal Relations, AT&T), letter to Tim Marvin, March 12, 2015, http://consumersunion.org/wp-content/uploads/2015/04/ATT_Response_robocalls_0315.pdf; John F. Jones (VP Public Policy & Federal Legislative Affairs, CenturyLink), letter to Tim Marvin, March 16, 2015, http://consumersunion.org/wp-content/uploads/2015/04/CentryLink_response_robocalls_0315.pdf; Donna Epps (Vice President – Policy & Strategic Alliances, Verizon), letter to Tim Marvin, March 9, 2015, http://consumersunion.org/wp-content/uploads/2015/04/Verizon_Response_robocalls_0315.pdf.

[16] "Guide: Caller ID and Spoofing," Federal Communications Commission, last modified December 30, 2014, https://www.fcc.gov/guides/caller-id-and-spoofing.

[17] *Ringing off the Hook: Examining the Proliferation of Unwanted Calls, Before the United States Senate Special Comm. on Aging,* 114th Cong. at 6 (2015) (testimony of Henning Schulzrinne), http://www.aging.senate.gov/imo/media/doc/Schulzrinne_6_10_15.pdf.

[18] Federal Trade Commission, *National Do Not Call Registry Data Book FY 2014*, p. 4.

[19] Ibid., 5.

[20] Federal Trade Commission, "FTC DNC and Robocall Enforcement," provided to fact-checker Christine Young by Mitchell Katz, September 28, 2015.

[21] Federal Trade Commission, *National Do Not Call Registry Data Book FY 2014*, p. 4. Complaints about unwanted calls soared from almost 600,000 in 2004 to 3.2 million in 2014. In 2012, complaints reached a peak of 3.8 million.

[22] Bikram Bandy, "Your Top 5 Questions About Unwanted Calls and the National Do Not Call Registry," *Consumer Information* (blog), Federal Trade Commission, March 9, 2015, https://www.consumer.ftc.gov/blog/your-top-5-questions-about-unwanted-calls-and-national-do-not-call-registry.

[23] "National Do Not Call Registry," Federal Trade Commission, accessed September 21, 2015, https://www.donotcall.gov/.

[24] "Consumer Information: National Do Not Call Registry," Federal Trade Commission, accessed September 21, 2015, http://www.consumer.ftc.gov/articles/0108-national-do-not-call-registry.

[25] Federal Communications Commission, 47 CFR Parts 64 and 68, Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, 68 Fed. Reg. 44,144 (July 25, 2003) (to be codified at 47 C.F.R. Parts 64 and 68) http://www.gpo.gov/fdsys/pkg/FR-2003-07-25/pdf/03-18766.pdf.

[26] Federal Trade Commission, *National Do Not Call Registry Data Book FY 2014*, p. 4.

[27] Telemarketing Sales Rule, 16 C.F.R. § 310.4 (b)(iii)(B) (2015), http://www.ecfr.gov/cgi-bin/text-idx?SID=e5b3e8329fb5cd9f55fe0bf675199b5f&mc=true&node=pt16.1.310&rgn=div5.

[28] Consumers Union defines a "robocall" as an unsolicited call made with a computerized autodialer, featuring either a pre-recorded message or a live agent.

[29] 47 C.F.R. § 64.1200(a)(3) (2015), http://www.ecfr.gov/cgi-bin/text-idx?rgn=div6&node=47:3.0.1.1.11.12 (federal regulations place restrictions on pre-recorded calls to home and cellular phones. It is illegal for a telemarketer to place a pre-recorded call to a home phone without permission).

[30] C.F.R. § 64.1200(a)(1)(iii) (it is illegal for a telemarketer to autodial a wireless line without permission).

[31] Telemarketing Sales Rule, 16 C.F.R. § 310.2(o) on the definition of the "established business relationship," and Telemarketing Sales Rule, 16 C.F.R. § 310.4 (b)(iii)(B)(ii) on the exemption for an "established business relationship."

[32] 47 C.F.R. § 64.1200 (a)(1)(iii) (these types of autodialed calls are not permitted to cellular phones).

[33] "The Do Not Call Registry," Federal Trade Commission, accessed August 29, 2015, https://www.ftc.gov/news-events/media-resources/do-not-call-registry.

[34] Federal Communications Commission, *Declaratory Ruling and Order*, CG Docket No. 02-278, WC Docket No. 07-135 (2015), 66, https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-72A1.doc.

[35] Ibid., 63-4.

[36] Ibid., 65.

[37] Ibid., 71.

[38] "FTC Challenges Innovators to Do Battle with Robocallers: Agency Offers $50,000 for Best Technical Solution as Part of Ongoing Fight against Illegal Calls," Federal Trade Commission, October 18, 2012, https://www.ftc.gov/news-events/press-releases/2012/10/ftc-challenges-innovators-do-battle-robocallers.

[39] Henning Schulzrinne (Levi Professor of Computer Science and Electrical Engineering, Columbia University), in discussion with the author, June 4, 2015.

[40] Federal Trade Commission, "Robocalls: All the Rage," 234.

[41] Schulzrinne, discussion.

[42] Bikram Bandy, interview by Catherine Fredman, May 19, 2015.

[43] *Ringing off the Hook,* testimony of Henning Schulzrinne, 2.

[44] "Guide: Caller ID and Spoofing," Federal Communications Commission.

[45] Henning Schulzrinne, "Telephone Numbers in an IP Environment," (presentation, IETF 92, Dallas, TX, March 26, 2015), approximately 23:05, http://recordings.conf.meetecho.com/Playout/watch.jsp?recording=IETF92_MODERN&chapter=chapter_0.

[46] Federal Trade Commission, "Robocalls: All the Rage," 145.

[47] Ibid., 133.

[48] Eric Burger (Research Professor of Computer Science and Director, Georgetown Center for Secure Communications, Georgetown University), in discussion with Consumers Union's End Robocalls team, April 15, 2015.

[49] Bandy, interview.

[50] Ibid.

[51] *Ringing off the Hook,* testimony of Lois Greisman, p. 3, footnote 11.

[52] Schulzrinne, discussion.

[53] *IRS: TIGTA Update Part II: Before the United States House of Representatives Committee on Government Oversight and Reform,* 114th Cong. at 6 (2015) (testimony of J. Russell George and Timothy P. Camus, TIGTA), http://www.treasury.gov/tigta/congress/congress_06252015.pdf.

[54] Consumer story submitted to Consumers Union at https://stori.es/share/stop-the-robocalls-campaign-story-form.

[55] "FTC Sends Refund Checks Totaling More Than $700,000 to Consumers Who Lost Money in Robocall Scheme: More Than 16,500 Checks Are Being Mailed This Week," Federal Trade Commission, January 16, 2015, https://www.ftc.gov/news-events/press-releases/2015/01/ftc-sends-refund-checks-totaling-more-700000-consumers-who-lost.

[56] Colleen Tressler, "To Robocall Scammers Who Lied about Free Medical Alert Devices: We've Got Your Number," *Consumer Information* (blog), Federal Trade Commission, January 13, 2014, https://www.consumer.ftc.gov/blog/robocall-scammers-who-lied-about-free-medical-alert-devices-weve-got-your-number.

[57] "Tax Scams/Consumer Alerts," Internal Revenue Service, last modified August 21, 2015, http://www.irs.gov/uac/Tax-Scams-Consumer-Alerts.

[58] "CFPB Sues Participants in Robo-Call Phantom Debt Collection Operation: Bureau Also Obtains a Temporary Restraining Order to Halt Illegal Operation and Freeze Assets of Operation's Leaders," Consumer Financial Protection Bureau, April 8, 2015, http://www.consumerfinance.gov/newsroom/cfpb-sues-participants-in-robo-call-phantom-debt-collection-operation/.

[59] "Tech Support Scams," Federal Trade Commission, January 2014, http://www.consumer.ftc.gov/articles/0346-tech-support-scams; Edward Wyatt, "Multinational Crackdown on Computer Con Artists," *New York Times*, October 3, 2012, http://www.nytimes.com/2012/10/04/business/multinational-crackdown-on-computer-con-artists.html?_r=0.

[60] "Tax Scams/Consumer Alerts," Internal Revenue Service.

[61] Bikram Bandy, "Getting Calls from Your Own Number?" *Consumer Information* (blog), Federal Trade Commission, July 7, 2015, https://www.consumer.ftc.gov/blog/getting-calls-your-own-number.

[62] Payas Gupta, Bharat Srinivasan, Vijay Balasubramaniyan, Mustaque Ahamad, "Phoneypot: Data-driven Understanding of Telephony Threats," Internet Society, 2015, p. 1, http://www.internetsociety.org/sites/default/files/03_2_3.pdf.

[63] Schulzrinne, discussion; *Ringing off the Hook,* testimony of Henning Schulzrinne, 1.

[64] *Ringing off the Hook,* testimony of Henning Schulzrinne, 3.

[65] Ibid., 6.

[66] Federal Trade Commission, "Robocalls: All the Rage, An FTC Summit," 219.

[67] *Ringing off the Hook,* testimony of Henning Schulzrinne, 6.

[68] Ibid., 5.

[69] Aaron Foss (Inventor, Nomorobo), in discussion with Consumer Reports staff, March 31, 2015, Yonkers, NY.

[70] "Supported Carriers," Nomorobo, accessed September 21, 2015, https://www.nomorobo.com/signup.

[71] Foss, discussion.

[72] Aaron Foss, interview with the author, June 11, 2015.

[73] "M3AAWG Telephony Honeypots: Benefits and Deployment Options," Messaging, Malware and Mobile Anti-Abuse Working Group, August 2014, 2, https://www.m3aawg.org/sites/default/files/document/M3AAWG_Telephony_Honeypots_BP-2014-08.pdf.

[74] Schulzrinne, discussion.

[75] Payas Gupta (Research Scientist at New York University Abu Dhabi), in discussion with the author, June 3, 2015.

[76] Aaron Foss, interview, June 11, 2015.

[77] Aaron Foss, interview by Catherine Fredman, May 22, 2015.

[78] Aaron Foss, "Ask me Anything," *Reddit*, January 21, 2015, https://www.reddit.com/r/IAmA/comments/2sax3w/iama_guy_that_fights_phone_scammers_telemarketers/.

[79] Foss, discussion.

[80] Ibid.

[81] Consumer story submitted to Consumers Union at https://stori.es/share/tell-us-about-your-robocall-call-blocker.

[82] "Robocall-Blocker Review: Is There Any Way to Eliminate Those Maddening Calls?" *Consumer Reports*, last modified August 14, 2015, http://www.consumerreports.org/cro/magazine/2015/07/robocall-blocker-review/index.htm.

[83] Federal Trade Commission, "Robocalls: All the Rage, An FTC Summit," 219.

[84] Brad Fisher (Senior Vice President of Marketing and Product at Primus Telecommunications Canada, Inc.), in discussion with the author, June 24, 2015.

[85] Fisher, discussion

[86] Fisher, discussion.

[87] Herb Weisbaum, "Why Aren't Phone Companies Doing More to Stop Robocalls?" *CNBC,* July 17, 2013, http://www.cnbc.com/id/100887510.

[88] Fisher, discussion.

[89] Fisher, discussion.

[90] *Stopping Fraudulent Robocall Scams: Can More Be Done?, Before the United States Senate Subcomm. on Consumer Protection, Product Safety, and Insurance,*113th Cong. (2013) (statement of Matt Stein), http://www.gpo.gov/fdsys/pkg/CHRG-113shrg85765/html/CHRG-113shrg85765.htm.

[91] USTelecom, Detailed Response to Sen. McCaskill, p. 5, http://www.mccaskill.senate.gov/imo/media/doc/RobocallDetailedResponsetoSen%20McCaskill.pdf. Linked to "McCaskill Drafting Bill to Crack Down on Fraudulent Robocalls," Senator Claire McCaskill, December 4, 2013, http://www.mccaskill.senate.gov/media-center/news-releases/mccaskill-drafting-bill-to-crack-down-on-fraudulent-robocalls.

[92] Federal Communications Commission, *Declaratory Ruling and Order*, CG Docket No. 02-278, WC Docket No. 07-135 (2015), 73, https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-72A1.doc.

[93] *Ringing off the Hook,* (comments of Henning Schulzrinne, approximately 1:09:50).

[94] Ibid., approximately 58:48.

[95] Schulzrinne, discussion.

[96] *Ringing off the Hook,* testimony of Henning Schulzrinne, 6.

[97] Federal Communications Commission, "Workshop to Focus on Robocall Blocking and Caller ID Spoofing," September 16, 2015, Washington, DC (comments of Jerusha Burnett, FCC, approximately 217:12), https://www.fcc.gov/events/workshop-focus-robocall blocking-and-caller-id-spoofing.

[98] FCC, "Workshop," (comments of Adam Panagia, approximately 257:15).

[99] CTIA, "Blocking Robocalls," accessed September 4, 2015.

[100] Sharpe, discussion.

[101] "PrivacyStar: Block Calls and Caller ID," Google Play Store, accessed June 21, 2015, https://play.google.com/store/apps/details?id=com.privacystar.android&hl=en.

[102] Sasse, discussion.

[103] *Ringing off the Hook,* testimony of Henning Schulzrinne, 4.

[104] Schulzrinne, discussion.

[105] *Ringing off the Hook* (comments of Henning Schulzrinne, approximately 59:38).

[106] *Ringing off the Hook,* testimony of Henning Schulzrinne, 6.

[107] Sharpe, discussion; Sasse, discussion.

[108] Heather McCulligh, Broadreach Communications, representing Primus Canada, email message to the author, September 15, 2015.

[109] Fisher, discussion.

[110] Henning Schulzrinne, e-mail message to author, July 17, 2015.

[111] *Ringing off the Hook* (comments of Henning Schulzrinne, approximately 1:10:35).

[112] *Ringing off the Hook,* (comments of Henning Schulzrinne, approximately 1:10:45).

[113] Ibid., approximately 1:10:57.

[114] Sasse, e-mail message to author, October 5, 2015. These services are available on the Google Play store. See "Metro Block-it," Google Play, accessed October 6, 2015, https://play.google.com/store/apps/details?id=com.privacystar.android.metro&hl=en; "CallWatch-Boost/Virgin/Sprint," Google Play, accessed October 6, 2015, https://play.google.com/store/apps/details?id=com.privacystar.android.spg&hl=en; and "Call Detector," Google Play, accessed October 7, 2015, https://play.google.com/store/apps/details?id=com.privacystar.android.tracfone&hl=en, for products designed for MetroPCS, Boost, Virgin Mobile, Sprint Prepaid, and TracFone customers.

[115] Sasse, e-mail message to author, October 5, 2015. Sasse says that PrivacyStar also works with the top carriers on billing integration, so that consumers can pay for the apps through their phone companies.

[116] Evan Oei, email to fact checker Christine Young, September 23, 2015.

[117] Sharpe, discussion.

[118] Sasse, discussion.

[119] Ibid.

[120] Sharpe, discussion.

[121] Foss, interview, June 11, 2015.

[122] See Jyrki T.J. Penttinen, The Telecommunications Handbook: Engineering Guidelines for Fixed, Mobile and Satellite Systems (John Wiley & Sons, 2015), 219 for a discussion of "softswitches."

[123] Aaron Foss, interview with the author, September 1, 2015.

[124] *Ringing off the Hook,* testimony of Henning Schulzrinne, 4.

[125] USTelecom, Detailed Response, 10.

[126] *Ringing off the Hook,* testimony of Henning Schulzrinne, 6.

[127] Ibid., 7.

[128] Ibid.

[129] FCC, "Workshop," (comments of Henning Schulzrinne, approximately 238:20).

[130] FCC, "Workshop," (comments of Adam Panagia, approximately 239:40).

[131] Ibid., approximately 240:30.

[132] "About the IETF," IETF, accessed August 30, 2015, http://ietf.org/about/.

[133] "Charter for Working Group," Security Telephony Identity Revisited (stir), IETF, accessed August 30, 2015, https://datatracker.ietf.org/wg/stir/charter/ ; *Ringing off the Hook,* testimony of Henning Schulzrinne, 5.

[134] Hadriel Kaplan, email to stir at ietf.org, "[stir] Calling Name Identity Trust (CNIT) mailing list," August 27, 2013, http://www.ietf.org/mail-archive/web/stir/current/msg01500.html.

[135] The IETF group is not the only organization working to address call spoofing. Martin C. Dolly of the Alliance for Telecommunications Industry Solutions (ATIS) says that his organization is working on a proposal. FCC, "Workshop," approximately 79:30.

[136] *Ringing off the Hook,* testimony of Henning Schulzrinne, 5.

[137] McKone, letter to Tim Marvin; Epps, letter to Tim Marvin.

[138] J. Scott Marcus, Richard Shockey, *Review of Resource Public Key Infrastructure (RPKI) to Verify Ownership and Authenticity of Telephone Caller ID over Voice over Internet Protocol*, June 10, 2015, p. 31, http://stakeholders.ofcom.org.uk/binaries/research/technology-research/2015/Ofcom_VoIP_RPKI_Report.pdf.

[139] *Ringing off the Hook,* testimony of Henning Schulzrinne, 5.

[140] Paul Hoffman, "What Is the IETF?" in *The Tao of IETF: A Novice's Guide to the Internet Engineering Task Force*, 2012, http://ietf.org/tao.html.

[141] Federal Communications Commission, *Report and Order, Order and Reconsideration, and Further Notice of Proposed Rulemaking*, GN Docket No. 13-5, RM-11358, WC Docket No. 05-25, RM-10593 at 170 (2015) (statement of Commissioner Mignon Clyburn) http://transition.fcc.gov/Daily_Releases/Daily_Business/2015/db0807/FCC-15-97A1.pdf.

[142] See Appendix for a description of AT&T, Verizon, and CenturyLink's call blocking offerings.

[143] Consumer story submitted to Consumers Union at https://stori.es/share/tell-us-about-your-robocall-call-blocker.

[144] For example, Verizon traditional landline service. Verizon representative, online chat with the author, August 6, 2015.

[145] For example, Verizon traditional landline service. Verizon representative, online chat with the author, August 6, 2015.

[146] "Use No Solicitation to Stop Sales Calls," CenturyLink, accessed August 30, 2015, http://www.centurylink.com/help/?assetid=287.

[147] CenturyLink representative, online chat with the author, September 22, 2015.

[148] Foss, discussion.

[149] "Call Blocking and Call Screening for U-verse Voice," AT&T, accessed August 30, 2015, http://www.att.com/esupport/article.jsp?sid=KB401019&cv=814&br=BR&ct=9000976&pv=2.

[150] "Incoming Call Block – FiOS Digital Voice," Verizon, accessed August 30, 2015, https://www.verizon.com/support/residential/phone/homephone/general+support/fios+voice+service/ad/129036.htm.

[151] "Telemarketer Block," Voipo, last modified January 30, 2014, http://www.voipo.com/help/article/telemarketer-block-70.html.

[152] "Nomorobo Partners with VOIPO to Protect Subscribers From Annoying and Illegal Robocalls: Nomorobo's Simple-to-Activate Service Is Now a Key Featured Offered to VOIPO's Existing Customer Base," *Yahoo! Finance,* July 8, 2014, http://finance.yahoo.com/news/nomorobo-partners-voipo-protect-subscribers-153929450.html.

[153] "CenturyLink Announces Virtualization Plans as it Continues Integrating its Network into the Cloud," CenturyLink, October 19, 2015, http://news.centurylink.com/news/centurylink-announces-virtualization-plans-as-it-continues-integrating-its-network-into-the-cloud.

[154] "Robocall Blocker Review: Is There Any Way to Eliminate Those Maddening Calls?" *Consumer Reports*, last modified August 14, 2015, http://www.consumerreports.org/cro/magazine/2015/07/robocall-blocker-review/index.htm.

[155] "Cordless Phones with Call Block," SmithGear.

[156] "Block Calls and Block or Filter Messages on Your iPhone, iPad, or iPod Touch," Apple.com, accessed September 1, 2015, https://support.apple.com/en-us/HT201229.

[157] "June 2015 Open Commission Meeting," Federal Communications Commission, June 18, 2015, approximately 2:17:00, https://www.fcc.gov/events/open-commission-meeting-june-2015, also available at https://www.youtube.com/watch?v=Jj9TrhUkWQc&index=3&list=PL1AEE1B8B41B867D3.

[158] Federal Communications Commission, *Declaratory Ruling and Order*, CG Docket No. 02-278, WC Docket No. 07-135, 108, (2015) (statement of Commissioner Mignon Clyburn) https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-72A1.doc.

[159] National Association of Attorneys General, letter to Randall Stephenson (AT&T), Lowell C. McAdam (Verizon), Glen F. Post, III (CenturyLink), Marcelo Claure (Sprint), John Legere (T-Mobile), July 22, 2015, http://www.oag.state.md.us/Press/NAAG_Call_Blocking.pdf.

[160] Sens. Edward J. Markey, Ron Wyden, Tammy Baldwin, Jeff Merkley, Richard Blumenthal, Elizabeth Warren, Al Franken, and Amy Klobuchar, letter to Tom Wheeler, August 5, 2015, http://www.markey.senate.gov/imo/media/doc/2015-08-15-TCPA-FCC.pdf

[161] Brad Gillen, "CTIA Statement in Response to Senator Blumenthal and Commissioner Rosenworcel Press Conference on Robocalls," *CTIA Blog*, July 13, 2015, http://blog.ctia.org/2015/07/13/ctiastatement-in-response-to-senator-blumenthal-and-commissioner-rosenworcel-press-conference-on-robocalls/.

[162] Jonathan Banks, "USTelecom Statement on FCC Robocall Order," USTelecom, June 18, 2015, http://www.ustelecom.org/news/press-release/ustelecom-statement-fcc-robocall-order.

[163] See, for example, Tim Marvin, letter to Lowell McAdam (Chairman and CEO of Verizon Communications, Inc.), February 17, 2015, http://consumersunion.org/research/letter-to-verizon-to-provide-consumers-free-solutions-to-block-robocalls/.

[164] Epps, letter to Tim Marvin; McKone, letter to Tim Marvin; Jones, letter to Tim Marvin.

[165] Epps, letter to Tim Marvin.

[166] Dave Lieber, "Let's Force Phone Companies to Stop Unwanted Calls," Dallas Morning News, last updated August 31, 2015, http://www.dallasnews.com/investigations/watchdog/20150829-lets-force-phone-companies-to-stop-unwanted-calls.ece; Karin Price Mueller, "Bamboozled: What Are Phone Companies Doing About Unwanted and Annoying Robocalls?" *NJ.com,* July 30, 2015, http://www.nj.com/business/index.ssf/2015/07/bamboozled_what_are_phone_companies_doing_about_un.html.

[167] Lieber, "Let's Force Phone Companies to Stop Unwanted Calls," *Dallas Morning News*.

[168] Federal Trade Commission, "Robocalls: All the Rage, An FTC Summit," 228.

[169] Mustaque Ahamad (Professor, College of Computing, Georgia Institute of Technology, and co-founder of Pindrop Security), in discussion with the author, May 28, 2015.

[170] Sharpe, discussion.

[171] Fisher, discussion.

[172] "Nomorobo Partners with VOIPO to Protect Subscribers From Annoying and Illegal Robocalls,"*Yahoo! Finance*.

[173] Ahamad, discussion.

[174] Sasse, discussion.

[175] Burger, discussion.

[176] Federal Trade Commission, "Robocalls: All the Rage," 155.

[177] "How to Use Call Block (*60) or Call Screening Features," AT&T, accessed August 30, 2015, http://www.att.com/esupport/article.jsp?sid=KB408880&cv=807&ct=9001834&pv=2

[178] AT&T representative, phone call with Karim Salamah, August 17, 2015. Includes Anonymous Call Blocking. Based on service to San Francisco, CA.

[179] "Call Blocking and Call Screening for U-verse Voice," AT&T.

[180] "List of U-verse Calling Features and Star Codes," AT&T, accessed August 30, 2015, http://www.att.com/esupport/article.jsp?sid=KB401850&cv=814.

[181] "Smart Limits," AT&T, accessed August 30, 2015, http://www.att.com/shop/wireless/smartlimits.html; "Smart Limits Terms and Conditions," AT&T, accessed August 30, 2015, http://www.att.com/legal/terms.smartLimitsTerms.html.

[182] "Call Blocking and Call Screening for U-verse Voice," AT&T.

[183] "How to Stop Unwanted Calls," AT&T, accessed August 30, 2015, http://www.att.com/esupport/article.jsp?sid=KB403232&cv=807. Options offered for AT&T local service are "Call Block, Call Trace, Call Return, and Anonymous Call Rejection."

[184] "Call Blocking and Call Screening for U-verse Voice," AT&T.

[185] "List of U-verse Calling Features and Star Codes," AT&T.

[186] "Blocking Calls and Messages to Your Wireless Phone," AT&T, accessed September 25, 2015, http://www.att.com/esupport/article.jsp?sid=KB102428&cv=820. Smart Limits plan is the only service option provided.

[187] "Privacy Manager User Guide," AT&T, accessed August 30, 2015, http://www.att.com/gen/general?pid=10211.

[188] AT&T representative, phone call with the author, August 4, 2015. Based on service in Oakland, CA.

[189] AT&T representative, online chat with the author, August 4, 2015.

[190] "Blocking Calls and Messages to Your Wireless Phone," AT&T. Smart Limits plan is the only service option provided.

[191] "List of U-verse Calling Features and Star Codes," AT&T.

[192] AT&T representative, phone call with Karim Salamah, August 17, 2015. Includes Anonymous Call Blocking. Based on service to San Francisco, CA.

[193] "List of U-verse Calling Features and Star Codes," AT&T.

[194] "Blocking Calls and Messages to Your Wireless Phone," AT&T. Smart Limits plan is the only service option provided.

[195] "Do Not Disturb Feature for U-verse Voice," AT&T, accessed September 4, 2015. http://www.att.com/esupport/article.jsp?sid=KB401818&cv=814.

[196] "How to Stop Unwanted Calls," AT&T. Options offered for AT&T local service are "Call Block, Call Trace, Call Return, and Anonymous Call Rejection."

[197] "Do Not Disturb Feature for U-verse Voice," AT&T; "List of U-verse Calling Features and Star Codes," AT&T.

[198] "Blocking Calls and Messages to Your Wireless Phone," AT&T. Smart Limits plan is the only service option provided.

[199] "Call Trace (*57) User Guide," AT&T, accessed August 30, 2015, http://www.att.com/esupport/article.jsp?sid=KB403269.

[200] AT&T representative, phone call with the author, September 23, 2015. Asked for general estimate.

[201] "Call Trace (*57) User Guide," AT&T.

[202] "Voice User Guide," AT&T, accessed August 30, 2015, http://www.att.com/media/att/2012/support/pdf/voice_user_guide.pdf; AT&T representative, online chat with the author, September 28, 2015.

[203] "Blocking Calls and Messages to Your Wireless Phone," AT&T. Smart Limits plan is the only service option provided.

[204] "FiOS Digital Voice Features," Verizon, accessed October 6, 2015, http://www.verizon.com/home/phone/fiosdigitalvoice/%20-%20features

[205] "Call Block," Verizon, accessed August 30, 2015, https://www.verizon.com/support/residential/phone/homephone/calling+features/call+block/call+block.htm. Available to new customers, also depending on area.

[206] Verizon representative, online chat with the author, August 6, 2015. This is an approximate estimate. Southern California residents pay $11.95 per month, according to a Verizon representative, phone call with Karim Salamah, August 18, 2015.

[207] "Incoming Call Block – FiOS Digital Voice," Verizon.

[208] "FiOS Digital Voice Features," Verizon, accessed October 6, 2015, http://www.verizon.com/home/phone/fiosdigitalvoice/%20-%20features.

[209] "Block Calls and Messages," Verizon, accessed August 30, 2015, https://wbillpay.verizonwireless.com/vzw/nos/safeguards/SafeguardProductDetails.action?productName=callMessa

geBlocking ; "Usage Controls - Manage Blocked Contacts," Verizon, August 30, 2015, http://www.verizonwireless.com/support/block-numbers/.

[210] Verizon representative, phone call with the author, August 31, 2015.

[211] Verizon representative, online chat with the author, August 6, 2015.

[212] "FiOS Digital Voice Features," Verizon, accessed August 30, 2015, http://www.verizon.com/home/phone/fiosdigitalvoice/%20-%20features; Verizon representative, phone call with Karim Salamah, August 18, 2015.

[213] Verizon representative, phone call with the author, August 31, 2015.

[214] "Call Trace," Verizon, accessed August 30, 2015, https://www.verizon.com/support/residential/phone/homephone/calling+features/call+trace/call+trace.htm.

[215] Verizon representative, online chat with the author, August 6, 2015.

[216] Verizon representative, phone call with Karim Salamah, August 18, 2015.

[217] Verizon representative, phone call with the author, July 17, 2015.

[218] "Do Not Disturb," Verizon, accessed August 30, 2015, https://www.verizon.com/support/residential/phone/homephone/calling+features/do+not+disturb/do+not+disturb.htm.

[219] Verizon representative, phone call with the author, August 6, 2015. This service is being grandfathered. This price is based on Pennsylvania.

[220] "FiOS Digital Voice Features," Verizon.

[221] "Block Calls and Messages," Verizon; "Usage Controls - Manage Blocked Contacts," Verizon. Do Not Disturb is not included in the offerings.

[222] "Home Phone Plans," CenturyLink, accessed October 6, 2015, http://www.centurylink.com/home/phone/

[223] "Ways to block unwanted calls from your home phone," CenturyLink, accessed August 30, 2015, http://www.centurylink.com/help/help/index.php?assetid=183.

[224] "Use Call Rejection to Block Calls You Don't Want," CenturyLink, accessed October 6, 2015, http://www.centurylink.com/help/?assetid=289.

[225] CenturyLink representative, online chat with the author, October 7, 2015. Based on Seattle.

[226] "Ways to block unwanted calls from your home phone," CenturyLink.

[227] CenturyLink representative, online chat with the author, September 23, 2015. Estimate.

[228] CenturyLink representative, online chat with the author, July 22, 2015. Based on Seattle.

[229] "Ways to block unwanted calls from your home phone," CenturyLink.

[230] CenturyLink representative, phone call with the author, August 7, 2015. Based on Seattle.

[231] CenturyLink representative, phone call with the author, August 31, 2015. Based on Seattle.

[232] Ibid.

[233] Ibid.

[234] "How to Use Calling Features to Block Unwanted Calls," CenturyLink, accessed August 30, 2015, http://www.centurylink.com/help/?assetid=233.

[235] CenturyLink representative, online chat with the author, July 22, 2015. Based on Seattle.

[236] "How to Use Calling Features to Block Unwanted Calls," CenturyLink.

[237] CenturyLink representative, phone call with Karim Salamah, August 27, 2015. Based on Seattle.

[238] CenturyLink representative phone call with the author, August 27, 2015, based on Seattle.

[239] CenturyLink representative, phone call with Karim Salamah, August 27, 2015. Based on Seattle.

[240] "Use No Solicitation to Stop Sales Calls," CenturyLink.

[241] CenturyLink representative, online chat with the author, July 22, 2015. Based on Seattle.