Relentless robocalls anger consumers

By Lauren Hall

Those automated telephone calls that deliver pre-recorded messages to your landline or cell phone—aka “robocalls”—are bombarding consumers’ devices at alarming rates. Consumers received a whopping 47 billion robocalls last year alone. Estimates are that nearly half of them were from scammers.

Unless you have explicitly consented to the calls, robocalls are generally prohibited under the federal Telephone Consumer Protection Act (TCPA), especially on cell phones. (Certain types of robocalls, such as political or charitable pitches, may be legal.)

But scammers and other disreputable calls don’t really care. For instance, a con artist will “spoof” (fake) the name and/or number on a phone’s call display to make it seem like the call’s coming from a government office (e.g., the IRS or Social Security Administration), a neighbor or even your own phone number! Spoofing legitimate numbers makes it more likely you will answer the phone and fall for the con. Caller ID spoofing software is widely available and can send thousands of calls for very little money.

Robocalling is a huge and growing problem: In 2017, seven million consumers complained to the Federal Communications Commission (FCC) and Federal Trade Commission (FTC) about robocalls. According to the FCC, robocalls make up 60 percent of all complaints it receives. The complaints have steadily increased despite the fact that consumers are taking what steps they can to protect themselves.

Consumers have placed more than 230 million phone numbers on the FTC’s Do Not Call Registry (https://www.donotcall.gov). Doing so prevents legitimate, untrevelled robocalls from ever reaching consumers’ phones.

Spoofed robocalls are an increasing problem for phone owners. These calls use fraudulent caller identification (Caller ID) information to disguise the caller’s true identity. For instance, a con artist will “spoof” (fake) the name and/or number on a phone’s call display to make it seem like the call’s coming from a government office (e.g., the IRS or Social Security Administration), a neighbor or even your own phone number! Spoofing legitimate numbers makes it more likely you will answer the phone and fall for the con. Caller ID spoofing software is widely available and can send thousands of calls for very little money.

Robocalling is a huge and growing problem: In 2017, seven million consumers complained to the Federal Communications Commission (FCC) and Federal Trade Commission (FTC) about robocalls. According to the FCC, robocalls make up 60 percent of all the complaints it receives. The complaints have steadily increased despite the fact that consumers are taking what steps they can to protect themselves.

Lawmakers throw down the gauntlet on robocalls

By Ruth Susswein

The Federal Communications Commission (FCC) estimates that nearly half (46%) of all robocalls are from scammers. All parties, including representatives from the telecom industry, are looking for lawmakers to get tough on illegal robocalls. New laws may be an easy lift, but we’ll be effective against out-and-out scammers remains to be seen.

Unlike with many other issues, the U.S. Congress has united around its desire to find useful ways to combat the unwanted automated calls popularly referred to as “robocalls.” In April, the Senate Commerce Committee unanimously approved legislation that would provide consumers with some relief from fraudulent, untrevelled robocalls.

While innovative approaches to stopping the scourge of illegal robocalls are more than welcome, it must be acknowledged that slightly more than half of robocalls are from legitimate businesses. The National Consumer Law Center’s Margot Saunders says that companies making legitimate robocalls would largely be spared in some of the legislation being considered by Congress, but points out that legitimate businesses making illegal calls to cell phones without consent is a major reason 2018 was the worst year on record for robocalls.

TRAncED Act (S.151): The Telephone Robocall Abuse Criminal Enforcement and Deterrence (TRAncED) Act would require telephone companies to adopt technologies for authenticating calls and alert consumers if an incoming call was from a “spoofed” (faked) number. (Depending on your carrier, it may say “Suspicious” or “Spam!” before the incoming number on Caller ID.)

This technology is called STIR/SHAKEN (Secure Telephone Identity Revisited, or STIR, and Signature-based Handling of Asserted Information using toKENs, or SHAKEN). In May, FCC chief Ajit Pai called on phone carriers to hurry up and voluntarily implement the call authentication system by the end of 2019, or be forced to do so by the commission.

The TRACED Act would give the FCC—the nation’s telecom regulator—more time and authority to take enforcement action against robocall violators. Currently, the FCC can only take action against robocallers for one year from when the call was placed. The TRACED Act would extend that time to three years, as well as require the FCC to craft rules to help prevent calls or texts with spoofed numbers from ever reaching consumers’ phones. It also would broaden the enforcement authority of the Federal Trade Commission (FTC).

The TRACED Act would allow for increased penalties for intentional violations of telemarketing regulations, up to $10,000 per robocall. If the intentional violations continued, the fine could jump to $30,000 per call. The bill calls for civil penalties for legitimate businesses that repeatedly call numbers that have been recycled (“reasigned”) to other customers or simply repeatedly flout the law. The bill would extend the window for the FCC to catch and take civil enforcement action against intentional violations from one to three years after a robocall is placed. The bill also eliminates a requirement that the FCC warn companies before bringing an enforcement action against them if they subsequently skirt the law. State attorneys general across the country support the TRACED Act.

Another bill, the Robocall Enforcement Enhancement Act (S.2694), would extend the time the FCC has to pursue robocall and Caller ID spoofing violations, and would authorize the agency to act without the currently required warning.
Lawmakers

Continued from page 1

StopPA is a bill for the state's anti-spam robocall law. Massachusetts's bill would bar robocalls to cell phones (under state law) and increase penalties to $10,000 per violation, and New Jersey lawmakers launched a bill to force robocallers to provide free robocall blocking for cellphones and landlines. In reality most of these measures would do no good: During March, $660 million in robocall complaints were filed with the Federal Communications Commission (FCC).

State legislation

While Congress and the FCC consider how to solve the relentless robocall problem, state lawmakers are busy coming up to combat this growing harm.

Caller ID spoofing ban (SB 208): This bill before the California State Senate sets a deadline for telecoms to prevent “neighbor spoofing” — displaying Caller ID numbers that appear to be local calls, from the same area code and phone number. The bill would enable consumers to request that the phone company verify that Caller ID is accurate (with exceptions for medical offices and domestic abuse shelters, among other select entities). It would also allow people to give companies the right to use a phone company that violates the law.

Revolving robocall trends

The Telephone Consumer Protection Act (TCPA) limits the use of automated dialing systems, prerecorded messages, texts, faxes and telemarketing sales calls. Outside of emergency warnings, recorded messages and automated calls and texts to your cell or residential phone are forbidden without your written consent. (However, if you have not added their numbers to the Do Not Call Registry (https://www.donotcall.gov), prior consent is not required when sales calls are made manually and do not feature prerecorded messages.) Under the TCPA, without your written consent, companies may make this call only between 8 a.m. or after 9 p.m., or fail to provide the name of the company from which, or on whose behalf, they are calling. (Learn more: https://www.donotcall.gov/)."

The FCC created rules to implement the TCPA and established the Do Not Call Registry, which allows consumers to register their landline and cellphone numbers at https://www.donotcall.gov or 888-382-1222, at no charge. Marketers are prohibited from calling numbers on the Do Not Call list. If you can verify if your phone number is on the list or report unwanted calls to the FTC at the site. If you report a violation to the TCPA, consumers should document the illegal calls, including date, time, caller's identity and a summary of the call. (Voiceemails left on your phone can be used as proof, and marketers and scalpers are valuable documentation—use your mobile phone to re-record them and turn them into digital files.) Submit the information to the FCC and the FTC. This information is useful as proof in lawsuits against telemarketers or debt collectors. Consumers can recover up to $500 for each violation, and up to $1,500 if they can prove the TCPA was knowingly violated.

Debt collection rules

In May, the Consumer Financial Protection Bureau (CFPB) issued a new rule covering debt collectors that call borrowers seven times a week, and have one conversation per week—per debt—plus send one written text and email messages. There currently is no set limit on the number of debt collection calls allowed per day if they are made to block robocalls. The proposed changes would modify the 42-year-old Fair Debt Collection Practices Act.
Robocall combat tools

By Monica Steinisch

T

here has been enough of an outcry against robo-
calls and spam texts that service providers, app developers and inventors are finally provid-
ing some legitimate, effective op-
tions against the intrusions. Not all options work for all phones—some are carrier or device spe-
cific—but there’s sure to be some tool available that will give you some relief from the onslaught.

Do Not Call Registry

The Federal Trade Commis-
sion’s National Do Not Call Reg-
istry (https://www.donotcall.gov) is designed to reduce the number of unwanted telemarketing calls made to consumers’ home or mobile phones. There’s no cost to register your landline and mobile phone numbers.

Adding your number(s) to the list won’t stop calls from chari-
ties, political groups, debt collec-
tors, survey-takers or entities you already do business with, which you may find equally unwel-
coming, but it will put a dent in the total volume of unwanted calls.

The main shortcoming of the Do Not Call Registry is that the people who inundate consumers with unwanted robocalls gener-
ally are not particularly concerned with obeying the law. 

Call-blocking tools

Anonymous-call rejection is free and available regardless of which carrier provides your residential landline service. It’s easy to activate: Just listen for the calling tone and press *77 (touch-
tone phones) or dial 1177 (rotary
dial tone and press *77 (touch-
tone phones) or dial 1177 (rotary
dial tone and press *77 (touch-
tone phones) or dial 1177 (rotary
dial tone and press *77 (touch-
tone phones) or dial 1177 (rotary
dial tone and press *77 (touch-
tone phones) or dial 1177 (rotary
dial tone and press *77 (touch-
tone phones) or dial 1177 (rotary
dial tone and press *77 (touch-
tone phones) or dial 1177 (rotary
dial tone and press *77 (touch-
tone phones) or dial 1177 (rotary
dial tone and press *77 (touch-
tone phones) or dial 1177 (rotary
dial tone and press *77 (touch-
tone phones) or dial 1177 (rotary
dial tone and press *77 (touch-
tone phones) or dial 1177 (rotary
dial tone and press *77 (touch-
tone phones) or dial 1177 (rotary
dial tone and press *77 (touch-
tone phones) or dial 1177 (rotary
dial tone and press *77 (touch-
tone phones) or dial 1177 (rotary
dial tone and press *77 (touch-
tone phones) or dial 1177 (rotary
dial tone and press *77 (touch-
tone phones) or dial 1177 (rotary
dial tone and press *77 (touch-
tone phones) or dial 1177 (rotary
dial tone and press *77 (touch-
tone phones) or dial 1177 (rotary
dial tone and press *77 (touch-
tone phones) or dial 1177 (rotary
dial tone and press *77 (touch-
tone phones) or dial 1177 (rotary
dial tone and press *77 (touch-
tone phones) or dial 1177 (rotary

consumer’s permission to ro-

consumer’s permission to ro-

consumer’s permission to ro-

consumer’s permission to ro-

consumer’s permission to ro-

consumer’s permission to ro-

consumer’s permission to ro-

consumer’s permission to ro-

consumer’s permission to ro-

Consumer Action News • Spring 2019 • Page 3
When telemarketing protections don’t apply
Some robocalls, texts and prerecorded calls are allowed

By Alegra Howard

If the volume of unwanted robocalls and scam texts reaching your phone lines has mushroomed, you’re not alone. Many are from illegal scammers, but the calls and texts can come from companies and organizations that are exempt from the Telephone Consumer Protection Act (TCPA), a federal law that limits telemarketing calls and automated, prerecorded calls.

Legal exemptions

Placing your number on the Federal Trade Commission’s Do Not Call list (https://www.donotcall.gov) is intended to prohibit sales calls, but businesses can still legally contact you with prerecorded messages as long as they don’t try to sell you something. Messages from an airline about a flight cancellation, appointment reminders from your doctor, and pharmacies reminding you to refill your prescription all may legally contact you through the Do Not Call list. If they fail to do so, you can complain to the Federal Trade Commission (https://www.ftccomplaintassistant.gov).

Phone calls and texts from campaigns are legal, but there are a few restrictions. The last few years have seen an uptick in campaigns using texting as a way to rally support for candidates. From donation requests to election day reminders, political texts are the biggest trend on the campaign trail. With the 2020 campaign season right around the corner, consumers may wonder what rights they have to stop the barrage of communications from candidates.

Charities and non-profits

Prerecorded calls made by (or on behalf of) a non-profit organization to landlines for fundraising or informational purposes are allowed—even if your name is on the Do Not Call list. However, the name of the organization and a return telephone number must be provided at the start of the message. Non-profits and politicians may not robocall or text your cell phone unless you have given prior consent (written or oral). You could be giving consent when you sign up to volunteer, receive a newsletter, or make a donation, so double-check which “I agree” boxes have been checked before submitting your contact information. Be aware that individual, manually dialed calls from non-profit staff are still allowed to your cell phone.

To stop non-profits and campaigns from calling you, ask to be placed on the organization’s own do-not-call list. This also applies to third-party telemarketers calling on behalf of a charity. If any company or charity fails to stop calling, you can complain to the Federal Trade Commission.

Before you donate to a charity, make sure to check its donor privacy policy to see if your contact information might be sold to other organizations. Sites like the Better Business Bureau’s Give.org (http://www.give.org) and Charity Navigator (https://www.charitynavigator.org) provide an overview of an organization’s donor privacy standards (when available) if you’re unable to find it on the charity’s website.

Political campaigns

Phone calls and texts from campaigns are legal, but there are a few restrictions. The last few years have seen an uptick in campaigns using texting as a way to rally support for candidates. From donation requests to election day reminders, political texts are the biggest trend on the campaign trail. With the 2020 campaign season right around the corner, consumers may wonder what rights they have to stop the barrage of communications from candidates.

Campaigns usually obtain registered voters’ phone numbers from voter registration files, which are public. While political campaigns legally can autodial or send prerecorded calls to your landline without your consent, it is illegal for campaigns to use an automated dialing system to mass call or text your cell phone without your consent.

You might be wondering, then, why you are receiving so many campaign text messages that you’ve never consented to. There’s a loophole in the TCPA’s protection against unsolicited text messages—peer-to-peer texting (https://tweety.com/ftc/stop). This technology allows a campaign staffer or volunteer to send a large number of unsolicited text messages without recipient consent. As long as staffers have to press a send button each time they send a text, the system technically isn’t automated, even if a staffer contacts 1,000 voters per day.

You have the right, at any time, to opt out of receiving automated or prerecorded calls and texts to your cell phone. Once you ask, the campaign must place your number on its own do-not-call list. If they fail to do so, report it to the FTC (https://www.ftccomplaintassistant.gov).

Another annoying but legal practice is campaigns that sell supporters’ personal information to other campaigns and political organizations. During the 2016 GOP presidential primary campaign, nearly every presidential candidate sold supporter data for big money.

A CNN Money analysis of 2016 Federal Election Commission records found that by selling supporter lists, Marco Rubio made $504,651, Rand Paul pulled in $212,495 and former Wisconsin Governor Scott Walker made $142,757. Democratic campaigns run by Barack Obama and Hillary Clinton made millions from sharing their supporter lists after past elections.

So, what can you do to stop your data from being sold? When you donate or register with a campaign, the fine print may state that the campaign is able to sell your information. Opt out by asking each campaign to place you on its own do-not-call list.

Detecting fraud

If you suspect you’re receiving calls or texts from a scammer posing as a charity or political campaign, hang up and immediately report the communication to the Federal Trade Commission (https://www.ftccomplaintassistant.gov).

If you suspect a scam, don’t respond to any instructions such as “press X for” or “reply with X” if the message says it is to get more information. Pressing a number may be considered consent to use and sell your phone number to another company. It also lets scammers know they have a live line. Similarly, if you think you are dealing with a scammer, don’t respond to the suspicious text with “STOP” as you might when unsubscribing from a legitimate company’s marketing texts.

Lastly, be wary of any calls or texts that ask you for personal information, like your Social Security or driver’s license number, birth date, address or account information. Also, be wary of any official-looking but suspicious text with “STOP,” as it is to get more information. Pressing a number may be considered consent to use and sell your phone number to another company. It also lets scammers know they have a live line. Similarly, if you think you are dealing with a scammer, don’t respond to the suspicious text with “STOP” as you might when unsubscribing from a legitimate company’s marketing texts.

Charities and non-profits

Prerecorded calls made by (or on behalf of) a non-profit organization to landlines for fundraising or informational purposes are allowed—even if your name is on the Do Not Call list. However, the name of the organization and a return telephone number must be provided at the start of the message. Non-profits and politicians may not robocall or text your cell phone unless you have given prior consent (written or oral). You could be giving consent when you sign up to volunteer, receive a newsletter, or make a donation, so double-check which “I agree” boxes have been checked before submitting your contact information. Be aware that individual, manually dialed calls from non-profit staffers are still allowed to your cell phone.

To stop non-profits and campaigns from calling you, ask to be placed on the organization’s own do-not-call list. This also applies to third-party telemarketers calling on behalf of a charity. If any company or charity fails to stop calling, you can complain to the Federal Trade Commission.

Before you donate to a charity, make sure to check its donor privacy policy to see if your contact information might be sold to other organizations. Sites like the Better Business Bureau’s Give.org (http://www.give.org) and Charity Navigator (https://www.charitynavigator.org) provide an overview of an organization’s donor privacy standards (when available) if you’re unable to find it on the charity’s website.

Political campaigns

Phone calls and texts from campaigns are legal, but there are a few restrictions. The last few years have seen an uptick in campaigns using texting as a way to rally support for candidates. From donation requests to election day reminders, political texts are the biggest trend on the campaign trail. With the 2020 campaign season right around the corner, consumers may wonder what rights they have to stop the barrage of communications from candidates.

Campaigns usually obtain registered voters’ phone numbers from voter registration files, which are public. While political campaigns legally can autodial or send prerecorded calls to your landline without your consent, it is illegal for campaigns to use an automated dialing system to mass call or text your cell phone without your consent.

You might be wondering, then, why you are receiving so many campaign text messages that you’ve never consented to. There’s a loophole in the TCPA’s protection against unsolicited text messages—peer-to-peer texting (https://tweety.com/ftc/stop). This technology allows a campaign staffer or volunteer to send a large number of unsolicited text messages without recipient consent. As long as staffers have to press a send button each time they send a text, the system technically isn’t automated, even if a staffer contacts 1,000 voters per day.

You have the right, at any time, to opt out of receiving automated or prerecorded calls and texts to your cell phone. Once you ask, the campaign must place your number on its own do-not-call list. If they fail to do so, report it to the FTC (https://www.ftccomplaintassistant.gov).

Another annoying but legal practice is campaigns that sell supporters’ personal information to other campaigns and political organizations. During the 2016 GOP presidential primary campaign, nearly every presidential candidate sold supporter data for big money.

A CNN Money analysis of 2016 Federal Election Commission records found that by selling supporter lists, Marco Rubio made $504,651, Rand Paul pulled in $212,495 and former Wisconsin Governor Scott Walker made $142,757. Democratic campaigns run by Barack Obama and Hillary Clinton made millions from sharing their supporter lists after past elections.

So, what can you do to stop your data from being sold? When you donate or register with a campaign, the fine print may state that the campaign is able to sell your information. Opt out by asking each campaign to place you on its own do-not-call list.

Detecting fraud

If you suspect you’re receiving calls or texts from a scammer posing as a charity or political campaign, hang up and immediately report the communication to the Federal Trade Commission (https://www.ftccomplaintassistant.gov).

If you suspect a scam, don’t respond to any instructions such as “press X for” or “reply with X” if the message says it is to get more information. Pressing a number may be considered consent to use and sell your phone number to another company. It also lets scammers know they have a live line. Similarly, if you think you are dealing with a scammer, don’t respond to the suspicious text with “STOP” as you might when unsubscribing from a legitimate company’s marketing texts.

Lastly, be wary of any calls or texts that ask you for personal information, like your Social Security or driver’s license number, birth date, address or account information. Also, be wary of any official-looking but suspicious text with “STOP,” as it is to get more information. Pressing a number may be considered consent to use and sell your phone number to another company. It also lets scammers know they have a live line. Similarly, if you think you are dealing with a scammer, don’t respond to the suspicious text with “STOP” as you might when unsubscribing from a legitimate company’s marketing texts.