Political Robocalls and Robotexts are finally a target of the FCC

November 6, 2018

If you answer the phone and hear a recorded message instead of a live person, it's a robocall. Internet-powered phone systems have made it cheap and easy for scammers to make illegal sales robocalls from anywhere in the world. It also lets them hide from law enforcement by displaying fake caller ID information.

While industry has been making progress implementing consumer protections against robocalls, success for consumers requires sustained investment in a next-generation call authentication standard. Last month, 35 state attorneys general issued a joint letter (PDF) urging the federal government, specifically the Federal Communications Commission (FCC), to curtail illegal robocalls nationally. If industry starts to fall behind, the OCC believe that the FCC must implement a realistic call-authentication framework to combat spoofed robocalls to erode the ability of scam artist callers to trick consumers into answering their phones for calls they clearly do not want by illegally spoofing their Caller ID.

As the 2018 election period has demonstrated, many consumers have been deluged with an avalanche of wireless and wireline calls and/or texts from and about political campaigns. This flood isn't the only source of robocalls calls and robotexts, of course, they are also often used to solicit customers for timeshare opportunities and other sales promotions, but during election seasons the amount of funding directed at consumer outreach results in an overwhelming number of calls.

The FCC acted earlier this week directly with the telecom companies

On November 5, 2018, FCC Chairman Ajit Pai demanded that the telecom industry adopt a robust call authentication system to combat illegal caller ID spoofing and launch that system no later than next year. The technical name of call blocking is "call authentication" and the FCC has finally focused on making relief from the daylong parade of automated political solicitations a reality.

While general consumer protections against such calls exist to some degree through protections provided by the FCC and the U.S. Federal Trade Commission through its National Do Not Call Registry to provide call-blocking technology, the FCC has expressly implemented strict rules about political calls or texts.

While laws and rules exist, these types of calls are on the rise and the AGs requested that the FCC further strengthen rules to let telecommunications service providers block certain categories of robocalls, specifically spoofed calls. Robotexts - text messages generated through autodialing - are considered a type of call and fall under all robocall rules. Scammers use "spoofing" to hide their identities, by indicating that an incoming call from an unknown phone number may seem familiar: calls may carry the consumer's area code and even the several digits of related to the consumer's phone number, a deception that may often cause an unwitting consumer to answer a call they really don't want to receive.

Chairman Pai directed letters to thirteen telecom companies, including incumbent local exchange carriers like Frontier, cable operators like Comcast, the national wireless companies, and edge providers such as Google and the virtual telephone company bandwidth.com. The FCC directed a series of questions at the telecom providers pointedly requesting them to provide the FCC with dates and scope of "concrete plans to implement a robust call authentication framework," in order to "combat and stop originating and terminating illegally spoofed calls on your network."

For instance, in Pai's letter to Dan McCarthy, president and chairman of Connecticut-based local exchange carrier Frontier Communications, Chairman Pai stated that Commission staff had alerted him that Frontier had not yet developed a call blocking system, and Pai requested a detailed response be filed by Frontier (and the other telecom providers in letter to them) with the FCC by November 19, 2018.

The SHAKEN/STIR technical process should be promptly implemented

For a number of years, the OCC was a consumer advocate representative on the North American Numbering Council (NANC), a Federal Advisory Committee created to advise the Commission on numbering issues and to make recommendations that foster efficient and impartial number administration. This past May 2018, Chairman Pai accepted the recommendations of the NANC for implementing "SHAKEN/STIR," a technical framework that causes calls traveling through interconnected phone networks to be "signed" as legitimate by originating carriers and validated by other carriers before reaching consumers. The framework digitally validates the handoff of phone calls passing through the complex web of

networks, allowing the phone company of the consumer receiving the call to verify that a call is from the person supposedly making it.

With a robust framework in place, consumers and law enforcement alike could more readily identify the source of illegal robocalls and reduce their impact. And the Commission is considering additional actions—such as authorizing voice providers to block the delivery of unsigned or improperly signed calls to consumers—that would stem the flow of illegally spoofed robocalls to American consumers.

Additional information

For additional information, consumer tips and FAQs about robocalls and robotexts, along with web resources about call blocking, visit fcc.gov/robocalls.

2018-1026 FCC Rules for Political Robocalls and Robotexts Explained

If you feel you've received an illegal robocall or robotext, you can file a complaint with the FCC. Information about the FCC's informal complaint process, including how to file a complaint, and what happens after a complaint is filed, is available in the FCC Complaint Center FAQ.

Please visit OCC's website.