

TABLE OF CONTENTS

	Page
INTRODUCTION AND SUMMARY	1
DISCUSSION.....	3
I. THE COMMISSION SHOULD EXPAND THE SCOPE OF THE CURRENT SAFE HARBOR TO INCLUDE NETWORK-LEVEL BLOCKING AND SHOULD CONSIDER OTHER WELL-DEFINED FORMS OF REASONABLE BLOCKING.....	3
II. THE COMMISSION SHOULD ENSURE THAT REDRESS PROCEDURES ARE REALISTIC AND FAIR TO ALL PARTIES	6
III. THE COMMISSION SHOULD GIVE PROVIDERS FLEXIBILITY WHEN PRODUCING BLOCKED CALL LISTS	7
IV. THE COMMISSION SHOULD TAKE OTHER MEASURES TO PROTECT CONSUMERS WITHOUT IMPOSING UNNECESSARY BURDENS	9
CONCLUSION.....	11

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554**

In the Matter of)
)
Advanced Methods to Target and Eliminate) CG Docket No. 17-59
Unlawful Robocalls)

COMMENTS OF COMCAST CORPORATION

Comcast Corporation (“Comcast”) submits these comments in response to the Fourth Further Notice of Proposed Rulemaking released on July 17, 2020 in the above-captioned proceeding.¹

INTRODUCTION AND SUMMARY

Comcast strongly supports the Commission’s continuing efforts to reduce the problem of illegal and fraudulent robocalls. In recent years, the Commission has pursued a variety of important measures, in close coordination with voice service providers, to facilitate efforts by providers to combat abusive calling practices and protect consumers. This *Fourth FNPRM* is yet another step forward as the Commission continues the critical work of empowering voice providers to implement effective call blocking tools.

The Commission’s adoption of the *Third Report and Order* in this proceeding has provided helpful additional clarity for voice providers as they work to mitigate abusive calling practices. By adopting safe harbors for blocking based on reasonable analytics incorporating call authentication information and for blocking calls from “bad actor” providers, voice providers

¹ *Advanced Methods to Target and Eliminate Unlawful Robocalls*, Third Report and Order, Order on Reconsideration, and Fourth Further Notice of Proposed Rulemaking, FCC 20-96 (rel. July 17, 2020) (“*Third Report and Order*” and “*Fourth FNPRM*”).

have greater assurance that these practices will not expose them to unwarranted liability.² Moreover, by beginning to clarify the process for addressing claims for erroneous blocking, the Commission has set the stage for effective communication between callers and voice providers.³ These new rules will enhance efforts to develop and tailor tools that effectively target and eliminate unwanted or illegal robocalls.

Moving forward, the Commission should adopt measures in response to the *Fourth FNPRM* that would continue this progress. To begin with, Comcast supports the proposal to adopt an additional safe harbor for network-level blocking based on reasonable analytics that incorporate call authentication information. Such a safe harbor would give providers additional certainty when implementing blocking measures that the Commission has already authorized—and the Commission should consider expanding this safe harbor to include other authorized, objective, and readily verifiable blocking methods.

Comcast also supports several of the Commission’s other proposals in the *Fourth FNPRM*. Comcast agrees that the Commission should provide additional clarity regarding the process for addressing claims from callers who feel their calls have been erroneously blocked. These redress rules should provide flexibility and fairness to all parties, as discussed in more detail below. The Commission should also proceed with its proposal to require providers to make blocked call lists available to consumers. In adopting this requirement, the Commission should ensure that providers have sufficient flexibility in providing these lists in a format and manner that works best for their services, and should not impose impractical obligations such as listing all calls blocked at the network level. Finally, the Commission should continue pursuing

² See *id.* ¶¶ 25-45.

³ See *id.* ¶¶ 51-59.

certain other proposals in the *Fourth FNPRM*, such as encouraging “know-your-customer” programs, that protect consumers without overly burdening voice providers.

DISCUSSION

I. THE COMMISSION SHOULD EXPAND THE SCOPE OF THE CURRENT SAFE HARBOR TO INCLUDE NETWORK-LEVEL BLOCKING AND SHOULD CONSIDER OTHER WELL-DEFINED FORMS OF REASONABLE BLOCKING

Comcast strongly supports the Commission’s proposal to extend the existing safe harbor to cover network-level blocking based on reasonable analytics that incorporate call authentication information.⁴ Network-level blocking is a powerful weapon in the fight against robocalls.⁵ When the Commission authorized network-level blocking in its *2017 Robocall Blocking Order*, it recognized three types of calls that are “highly likely to be illegal”: “(1) numbers that are invalid under the North American Numbering Plan (NANP); (2) numbers that have not been allocated by the North American Numbering Plan Administrator (NANPA) or the Pooling Administrator (PA) to any provider; and (3) numbers that the NANPA or PA has allocated to a provider, but are not currently used.”⁶ By implementing technology targeting these types of calls, a provider can block millions or even billions of robocalls the moment they reach the provider’s network. Comcast, for its part, blocked over 86 million of these types of calls at the network level in July 2020 alone.

Comcast also supports the additional protections the Commission has proposed to ensure the effectiveness of network-level blocking covered by the safe harbor. The Commission’s

⁴ See *Fourth FNPRM* ¶ 104.

⁵ See *Advanced Methods to Target and Eliminate Unlawful Robocalls*, Report and Order and Further Notice of Proposed Rulemaking, 32 FCC Rcd 9706 ¶ 26 (2017) (“*2017 Robocall Blocking Order*”) (noting the benefits of network-level blocking are “potentially enormous”).

⁶ *Id.* ¶ 18.

proposal to require network-level blocking to be “specifically designed to block calls that are highly likely to be illegal” and “managed with sufficient human oversight and network monitoring to ensure that blocking is working as intended” is consistent with Comcast’s approach and industry best-practices.⁷ Adopting this proposal would help protect consumers from illegal robocalls while safeguarding the calls consumers want.

The Commission has ample legal authority to include network-level blocking within the safe harbor. The Commission already has determined that its existing, pre-TRACED Act authority (including Sections 201(b), 202(a), 251(e), and 4(i) of the Communications Act of 1934, as amended) is sufficient to adopt the current safe harbor for other forms of blocking based on reasonable analytics using call authentication information.⁸ The Commission further determined that the TRACED Act “confirm[ed]” that authority.⁹ Given this prior analysis, the Commission plainly also has authority to adopt the proposed safe harbor for network-level blocking using call authentication information.

The Commission also should consider extending this safe harbor further to include other authorized, objective, and readily verifiable blocking methods. For example, many providers, including Comcast, offer Anonymous Call Rejection (“ACR”), which automatically rejects calls where the caller has chosen to prevent the display of the caller’s name and number. As of March 6, 2020, this feature has been enabled by default for all of Comcast’s Xfinity Voice users. And as the Commission recognized in the *Third Report and Order*, Comcast’s ACR tool works

⁷ *Fourth FNPRM* ¶ 104.

⁸ *Third Report and Order* ¶¶ 61, 123.

⁹ *Id.* ¶ 66.

effectively to block millions of unwanted calls bound for its customers.¹⁰ Indeed, the Commission not only has authorized providers to offer ACR, but has *required* it in certain cases.¹¹

Today, however, some providers may be hesitant to enable ACR tools—or may decide to discontinue them—fearing liability under the Act and the Commission’s rules in the event that a legitimate call is blocked by the tool.¹² Extending the safe harbor to cover this tool thus would give providers greater certainty in their efforts to reduce unwanted robocalls. Moreover, such a safe harbor would not present the same concerns that caused the Commission to decline to adopt a broader safe harbor in the *Third Report and Order*; this safe harbor would not “lack[] objective criteria” or “clear standards,”¹³ but would be based on an objective, widespread, and well-understood blocking technique. Additionally, ACR tools provide a very simple avenue for remedying any claims of over-blocking; a caller blocked by ACR receives a message informing it that its call was blocked, with instructions for remedying the situation (i.e., by removing the

¹⁰ See *Third Report and Order* ¶ 23 n.67.

¹¹ See, e.g., *Telecommunications Relay Services and Speech-to-Speech Services for Individuals with Hearing and Speech Disabilities*, Report and Order, Order on Reconsideration, and Further Notice of Proposed Rulemaking, 19 FCC Rcd 12475 ¶ 74 (2004) (stating that providers telecommunications relay services are “required” to offer “anonymous call rejection” to the extent technically possible).

¹² See, e.g., Letter of Patrick Halley, USTelecom, Matthew Gerst, CTIA, and Steve Morris, NCTA, to Marlene Dortch, Secretary, FCC, CG Docket No. 17-59, at 3 (Jan. 31, 2020) (“USTelecom/CTIA/NCTA Jan. 31 Letter”) (noting that, “[w]hile the Commission gave voice service providers authority to block calls, and consumers increasingly support their provider blocking calls on their behalf, providers hesitate to deploy robust call blocking solutions for fear of liability” (citations omitted)).

¹³ *Third Report and Order* ¶ 50.

blocking of caller identification information on the caller's outbound line). The Commission thus should consider such an expansion of its safe harbor in this proceeding.¹⁴

II. THE COMMISSION SHOULD ENSURE THAT REDRESS PROCEDURES ARE REALISTIC AND FAIR TO ALL PARTIES

Comcast has long supported the creation of redress procedures that allow consumers and businesses to correct erroneous blocking or labeling.¹⁵ Specifically, Comcast has advocated for measures under which voice providers would create a single point of contact for the reporting of incorrect blocking or labeling and for providers to take remedial action promptly and efficiently. Thus, consistent with this prior advocacy, Comcast supports the Commission's efforts to provide further clarification concerning communications regarding complaints of erroneous blocking or labeling.

Specifically, Comcast supports the Commission's proposal to require providers to "respond" to complaints about erroneous call blocking within one week.¹⁶ Such communication is important for ensuring that a caller knows that its complaint has been received and that its concerns are being investigated and considered in a timely fashion. At the same time, however,

¹⁴ The Commission has legal authority to adopt safe harbors that go beyond technologies that use call authentication information. While the TRACED Act's safe harbor provision refers to the use of call authentication information, the Commission already has concluded that the pre-TRACED Act provisions cited above, including Sections 201(b), 202(a), 251(e), and 4(i), supply the requisite authority for safe harbors from liability under the Communications Act and the Commission's rules. *Third Report and Order* ¶¶ 61-65, 123. Indeed, the TRACED Act specifically provides that "nothing in this section shall preclude the Commission from initiating a rulemaking pursuant to its existing statutory authority," thus confirming that it does not limit the Commission's broad, existing authority to adopt safe harbors. Pallone-Thune TRACED Act, S. 151, 116th Cong. § 4(d) (2019) ("TRACED Act"); *see also* USTelecom/CTIA/NCTA Jan. 31 Letter at 3 (explaining, in light of this language in the TRACED Act, that "the Commission can create a broad safe harbor under its existing authority").

¹⁵ *See* Comments of Comcast Corp., CG Docket No. 17-59, at 11 (filed Sept. 24, 2018); Comments of Comcast Corp., CG Docket No. 17-59, at 4-5 (filed Jan. 23, 2018).

¹⁶ *Fourth FNPRM* ¶ 108.

the Commission should refrain from setting a concrete timeline for *resolving* such complaints. The time to resolve a complaint depends on a variety of factors that are beyond a voice provider's control, including: the complexity of the complaint, the responsiveness of the complainant if follow-up is needed, the responsiveness of third parties to the extent the issues implicate those parties' services, the technical requirements and costs associated with implementing any necessary changes to the blocking program as a result of the complaints, and other factors.

Ultimately, the Commission should examine the reasonableness of the provider's efforts to resolve a dispute in good faith on a case-by-case basis, rather than setting arbitrary timelines for responding to and resolving complaints. Such an approach would be consistent with the Commission's observation in the *Third Report and Order* that the "amount of time" that may be "reasonable" for "investigat[ing] and resolv[ing] these blocking disputes" will "vary depending on the specific circumstances of the blocking and the resolution of the blocking dispute."¹⁷ The Commission has already rejected calls for "extensive" rules setting timetables for resolving disputes, finding that a "reasonableness" standard "strike[s] an appropriate balance between the legitimate needs of both callers and voice service providers."¹⁸ The Commission should reaffirm that conclusion here.

III. THE COMMISSION SHOULD GIVE PROVIDERS FLEXIBILITY WHEN PRODUCING BLOCKED CALL LISTS

Comcast also generally supports the Commission's proposal to "require terminating voice service providers to provide a list of individually blocked calls that were placed to a particular

¹⁷ *Third Report and Order* ¶ 55.

¹⁸ *Id.* ¶ 57.

number at the request of the subscriber to that number,”¹⁹ subject to certain clarifications discussed below. As the Commission notes in the *Fourth FNPRM*, such a requirement would be consistent with the TRACED Act, which “directs the Commission to ensure consumers are provided with ‘transparency and effective redress options’ for call-blocking services provided on either an opt-out or opt-in basis.”²⁰ Among other benefits, blocked call lists would assist consumers in determining whether to continue using blocking tools offered on an opt-in or opt-out basis, and would enable consumers to return calls that they may believe to have been legitimate.

If the Commission follows through with its proposal to require providers to make such lists available, the Commission should avoid micromanaging the process and allow providers to do so in the format and manner of their choosing. Some providers may have ready-built user portals or mobile apps with call history logs, while other providers may prefer custom-made lists that are mailed to the customer’s billing address. The complexity of billing systems and variations in provider capabilities counsels against rigid rules for the presentation of blocked number lists. Under a flexible standard, the Commission could focus on ensuring that consumers are able to review the required information regardless of how these solutions are delivered, and this flexibility would allow providers to focus on accuracy and completeness rather than on presentation.

The Commission also should exclude from this requirement any calls that are blocked at the network level pursuant to the *2017 Robocall Blocking Order*. Because these calls are blocked at the edge of a provider’s network, they never make it far enough to be associated with

¹⁹ *Fourth FNPRM* ¶ 111.

²⁰ *Id.* ¶ 110 (quoting TRACED Act § 10(b)).

a particular customer's call logs. If providers were forced to account for these calls on a per subscriber basis, it would substantially increase the difficulty of implementing network-level blocking solutions and disincentivize providers from offering this effective tool. Moreover, there would be little, if any, value to consumers from including such calls on blocked calls lists; these calls are facially invalid and, by definition, contain telephone numbers that cannot be called back even if the consumer wished to do so.

IV. THE COMMISSION SHOULD TAKE OTHER MEASURES TO PROTECT CONSUMERS WITHOUT IMPOSING UNNECESSARY BURDENS

The *Fourth FNPRM* also seeks comment on affirmatively requiring voice service providers to “implement effective measures to prevent new and renewing customers from using its network to originate illegal calls.”²¹ In Comcast's experience, one of the most effective ways of doing so is through a “know your customer” methodology that identifies any outbound-dialed telephone numbers with nuisance-calling characteristics and enables the provider to take remedial action as appropriate.

Comcast's “know your customer” methodology analyzes call pattern metrics (such as call duration and answer rate) and incorporates them into a “Robo Score” for problematic telephone numbers. Comcast also reviews information regarding complaints filed at the Commission and at the Federal Trade Commission associated with particular numbers in an attempt to detect problem callers. Comcast's implementation of this methodology is in keeping with its commitments under the principles agreed upon by state attorneys general and large voice providers in August 2019.²² These principles include commitments to “analyze and monitor

²¹ *Fourth FNPRM* ¶¶ 95, 102-103.

²² See *Anti-Robocall Principles* (2019), <https://www.ustelecom.org/wp-content/uploads/2019/08/State-AGs-Providers-AntiRobocall-Principles-With-Signatories.pdf>.

network traffic” to “identify and monitor patterns consistent with robocalls,” and to “investigate suspicious calls and calling patterns” by, among other things, terminating a party’s ability to originate, route, or terminate calls over the voice network.²³ The Commission may wish to consider whether programs like Comcast’s can be effectively implemented by other providers and, if so, encourage other providers to implement such programs in an efficient and effective manner for their individual networks.

The *Fourth FNPRM* also proposes to require providers to respond to traceback requests from the Commission, law enforcement, or the Traceback Consortium—another commonsense measure that Comcast supports.²⁴ The Commission has already indicated that responses to traceback requests from the Traceback Consortium are covered by Section 222(d)(2) of the Act, which allows voice providers to use, disclose, or permit access to customer proprietary network information “to protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services”²⁵—and should reaffirm that determination here. The Commission also should provide guidance to voice providers on how it expects them to process traceback requests that come from sources other than the Traceback Consortium, including verifying that such requests are legally valid. Notably, the Commission’s rules otherwise require providers to receive “appropriate legal

²³ *Id.*

²⁴ See *Fourth FNPRM* ¶¶ 96-97.

²⁵ 47 U.S.C. § 222(d)(2); see also *Implementing Section 13(d) of the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (TRACED Act)*, Report and Order and Further Notice of Proposed Rulemaking, 35 FCC Rcd 3113 ¶ 26 & n.59 (2020).

authorization” prior to releasing any call record information to law enforcement.²⁶ The Commission should consider clarifying that these same standards apply to traceback requests from law enforcement.²⁷

CONCLUSION

Comcast strongly supports the Commission’s continued efforts to address the scourge of illegal and fraudulent robocalls. With the measures discussed above, the Commission can continue to promote the implementation of effective and appropriately tailored call-blocking tools and other initiatives to protect consumers from abusive calling practices.

Respectfully submitted,

/s/ Mitch Rose

Matthew T. Murchison
Alexander L. Stout
LATHAM & WATKINS LLP
555 Eleventh Street, NW
Suite 1000
Washington, DC 20004

Mitch Rose
Beth A. Choroser
Regulatory Affairs

Francis M. Buono
Legal Regulatory

COMCAST CORPORATION
300 New Jersey Avenue, NW
Suite 700
Washington, DC 20001

Brian A. Rankin
Andrew D. Fisher
COMCAST CORPORATION
1701 JFK Boulevard
Philadelphia, PA 19103

August 31, 2020

²⁶ See 47 C.F.R. §§ 1.20002, 1.20004 (requiring “appropriate legal authorization,” defined to include a court order or authorization pursuant to 18 U.S.C. § 2518(7) or “any other relevant federal or state statute”).

²⁷ In Comcast’s experience, valid legal requests seeking traceback information typically come in the format of a civil investigative demand or subpoena.