Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Implications of Artificial Intelligence Technologies on Protecting Consumers from Unwanted Robocalls and Robotexts	)	**CG Docket No. 23-362**

Comments of
National Consumer Law Center on behalf of its low-income clients
Electronic Privacy Information Center
Consumer Action
Consumer Federation of America
National Association of Consumer Advocates
The National Consumers League
Public Knowledge
U.S. Public Interest Research Group
Bay Area Legal Aid
Jacksonville Area Legal Aid
Idaho Legal Aid Services
Indiana Legal Services, Inc.
Mid Minnesota Legal Aid
Legal Aid of Western Missouri
Montana Legal Services
Legal Aid of Nebraska
603 Legal Aid of New Hampshire
CAMBA Legal Services of New York
Western New York Law Center, Inc.
North Carolina Justice Center
Pennsylvania Utility Law Project
Community Legal Services of Philadelphia
Legal Aid Services of Oklahoma
Legal Aid Justice Center
Mountain State Justice of West Virginia
Legal Action of Wisconsin

October 10, 2024

Submitted by:

Margot Saunders
Carolyn Carter
National Consumer Law Center
1001 Connecticut Ave, NW
Washington, DC 20036
msaunders@nclc.org

Chris Frascella
Matthew Contursi
Electronic Privacy Information Center
1519 New Hampshire Ave, NW
Washington, DC 20036
frascella@epic.org

Table of Contents

Comments

Introduction and Summary

These comments, written by the **National Consumer Law Center** (NCLC), on behalf of its low-income clients, and the **Electronic Privacy Information Center**, are joined in by **24 additional national, state and local advocacy and legal aid programs listed on the title page of these comments and described in the Appendix**, regarding the Notice of Proposed Rulemaking (NPRM) and Notice of Inquiry (NOI) issued by the Federal Communications Commission (Commission or FCC) on August 8, 2024, relating to the use of artificial intelligence in unwanted robocalls and robotexts.[1]

We appreciate the thoughtfulness and concern for protecting subscribers shown in these proposals, especially the clarity provided in the Declaratory Ruling issued in February 2024 confirming "that the TCPA's restrictions on the use of 'artificial or prerecorded voice' encompass current AI technologies that generate human voices" and that "calls that use such technologies fall under the TCPA and the Commission's implementing rules, and therefore require the prior express consent of the called party to initiate such calls absent an emergency purpose or exemption."[2]

We also support the FCC's proposed definition of an AI-generated call.[3] However, as the NPRM and NOI recognize, there are still important concerns that need to be worked through to ensure that subscribers are appropriately protected when this AI technology is used. In **Section I**, we strongly support the FCC's twin proposals related to calls that include AI-generated technology: first, to require that before callers can make AI-generated calls that may employ interaction with the recipient, the callers must obtain explicit consent from called parties to receive calls that use this

---

[1] *In re* Artificial Intelligence Technologies on Protecting Consumers From Unwanted Robocalls, Notice of Proposed Rulemaking and Notice of Inquiry, CG Docket 23-362 (Rel. Aug. 8, 2024), *available at* https://docs.fcc.gov/public/attachments/FCC-24-84A1.pdf [hereinafter AI NPRM]. *See also In re* Implications of Artificial Intelligence Technologies on Protecting Consumers From Unwanted Robocalls and Robotexts, Proposed Rule, CG Docket No. 23–362, 89 Fed. Reg. 73,321 (Sept. 10, 2024), *available at* https://www.govinfo.gov/content/pkg/FR-2024-09-10/pdf/2024-19028.pdf.

[2] *See In re* Implications of Artificial Intelligence Technologies on Protecting Consumers from Unwanted Robocalls and Robotexts, Declaratory Ruling, CG Docket No. 23-362, at ¶ 2 (Rel. Feb. 8, 2024), *available at* https://docs.fcc.gov/public/attachments/FCC-24-17A1.pdf [hereinafter AI Declaratory Ruling].

[3] *See* AI NPRM, *supra* note 1 at ¶ 10.

technology; and second, that these AI-generated calls must include a disclosure at the beginning of each call that the call uses this technology.[4]

To ensure that callers will comply, we urge the FCC to tie these two requirements together by interpreting "consent" in this context to mean that when a subscriber consents to receive calls that use AI-generated technology, they are consenting only to receive calls that include the disclosure at the beginning of the call. This would mean that any call that includes AI-generated technology that does not include the disclosure will not have been consented to by the recipient.

We also explain that callers who have already received consent from a called party to send them artificial voice calls should be permitted to rely on that previously provided consent for AI-generated calls, so long as the recipient will have no, or only minimal, interaction with the AI in those calls, and the calls use a generic human voice, rather than that of a specific human being. If the voice of a particular human being is used for the calls, the recipient must have provided prior express consent to receive AI-generated calls from that specific person.

Moreover, for all calls that do anticipate interaction with the AI technology, as we explain, this in-call disclosure is essential to protect telephone subscribers from confusion and deception, especially in collection and telemarketing calls.

It is important that the Commission not treat all AI-generated calls differently based on the type of line to which the calls are made—to cell phones or to residential lines. In other words, there should be no exemptions allowed for a certain number of calls to residential lines without consent, as there are for some non-telemarketing calls.

It is also important that recipients of all of these calls be informed of an option to opt out of the calls in the future.

Finally, we support ensuring that texts that include AI-generated voices are included in the proposed rule.

Section II addresses the needs of persons with disabilities who use AI-generated technology to make their calls. We support the need to facilitate these calls, but we believe that the FCC does not have authority to exempt these calls when they are made to cell phones, because it would be impossible to ensure that these calls would be free to the end user, as required by the exemption

[4] *See id.* at ¶¶ 14-15.

authority. Instead, we believe that the FCC can provide protection for AI-generated calls by providing a definition of "artificial voice" to exclude a mechanical voice that is generated by an assistive device by a person with disabilities to transmit their words over the telephone. In this situation, the vocalization of the words should not be considered an "artificial voice" for purposes of the TCPA. The use of a digital assistive device should be treated the same as a physical, prosthetic implant. Both use technology to verbalize that person's words, and neither involves what the TCPA should consider an "artificial voice," even if the assistive device uses AI-generated technology to transmit the words into the telephone. The result is not an "artificial voice" that should trigger the TCPA's requirement for consent.

Section III responds to the Notice of Inquiry[5] related to the potential use of technologies that use AI to detect and respond to potentially fraudulent calls at either a network or device level. We oppose any use of these technologies on a network level for multiple reasons, the leading of which is that they would seriously impinge on individuals' privacy.

[5] *Id.* at IV, ¶¶ 35-46.

I. The Commission should require specific prior express consent for AI-generated calls, as well as a disclosure at the beginning of most AI-generated calls.

We support the Commission's proposed definition for AI-generated calls, but AI calls should be regulated based on the degree to which the AI may create a risk of harm or confusion for the recipient.

The FCC proposes to define "AI generated call" as—

> a call that uses any technology or tool to generate an artificial or prerecorded voice or a text using computational technology or other machine learning, including predictive algorithms, and large language models, to process natural language and produce voice or text content to communicate with a called party over an outbound telephone call.[6]

This proposed definition is broad, as it should be. It would cover all calls using this type of technology, regardless of the content of the call. This is an appropriate approach because it allows for further delineation between calls as needed to protect recipients.

Additionally, the Commission is right to recognize that there are substantial risks of confusion—if not outright deception—resulting from AI-generated calls.[7] The risk to recipients varies depending on how the artificial intelligence is used in the calls.

Accordingly, we propose that AI-generated calls be regulated based on the risk of harm and confusion that they may cause. There are three categories into which these calls fall, with different levels of consent and protections that should be applicable to the different categories:

1. Simple informational calls, using a generic voice, with minimal interaction with the recipient.
2. Informational calls which include the voice of a specific human being.
3. AI-generated calls in which the recipient is expected to interact with AI.

All AI-generated voices need not be treated in identical fashion; rather, the risk created by AI-generated calls should determine the extent of their regulation. We propose that the consent and disclosure requirements for AI-generated calls should be determined based on the risks of misunderstanding and deception that could be caused by the calls using the technology. At this point, we recommend that AI-generated calls be categorized into the three categories described

[6] *Id.* at ¶ 10.

[7] *Id.* at ¶ 10 n.32.

below. Depending on future developments, it may be appropriate to add to or change the categorizations and concomitant protections associated with those types of calls. Note that we are not including AI-generated calls made by persons with a disability, because—as explained in section II, *infra*—we believe those calls can be excluded from TCPA coverage altogether.

As noted by the Commission, texts are covered as calls for these purposes.[8] Since texts can include voice messages, this is an essential determination.

We also urge the Commission to make no new exemptions for AI-generated calls to either cell phones or residential lines. The Commission should treat all AI-generated calls the same, regardless of whether the calls are to cell phones or to residential lines, and regardless of the subject matter of the call.

We propose three categories for AI-generated calls:

1. **Simple informational calls,** using a generic voice, with minimal interaction with the recipient.

These are simple notice calls from doctors' offices and pharmacies and the like, alerting the called party that a prescription is ready, an appointment has been scheduled, etc. Or these calls are simple alerts or notification calls from banks and other financial institutions, providing a code to verify an online account sign-on, or alerting the recipient that a payment is required, notices from airlines that a plane has been delayed, and the like. In these calls, a) the artificial voice produced by the AI may sound like a real human, but it is a generic voice, not a voice purporting to be from a specific person, and b) there is little or no interaction expected from the recipient, other than possibly to press a digit to provide a simple response signifying that the recipient is keeping an appointment, cancelling it, or requesting a call back to make a change.

Recommendation: For informational calls that use only a generic human voice, prior express consent should continue to be required for these calls, as they include an artificial voice,[9] but a disclosure about the possibility of using an AI-generated voice in these calls is not necessary, and a disclosure during the call that AI is used also need not be provided.

---

[8] *Id.*

[9] *See* AI Declaratory Ruling, *supra* note 2, at ¶ 5.

2. **Simple informational calls,** using the voice of a *specific human being*, that precipitate only minimal interactive response.

A distinction must be made between calls that include a generic voice of a human being and calls that include an artificial voice purporting to be from a specific human being. If the voice used in calls is the voice of a specific person, even if only minimal interaction is required of the recipient, these calls should be considered legal only if the recipient provided prior express consent to receive calls with prerecorded or artificial voice *from that person*. As the long as the calls are, in fact, from that person, and created either by that person, or with the permission of that person, there is no deception involved. As the recipient has consented to receive calls from that person which include an artificial or prerecorded voice, then no more notice about the call is necessary, and an in-call disclosure need not be made.

For example, suppose a consumer purchased tickets from a ticket sales and distribution company for a Taylor Swift concert and, in the process, agreed to receive calls and texts that include artificial and prerecorded voice calls from that ticket distribution company. A call from that company that uses a generic voice announcing a new time for the concert would have been consented-to by the consumer, and that call would fall under category 1, requiring no more specific consent regarding AI-generation used in the call. But unless the ticket distribution company had consent from the consumers to make calls from Taylor Swift herself, the company could not use her voice to make those calls.

It is essential that the FCC require specific prior express consent for calls that purport to be from a real person to ensure that consumers are not misled about the source and reliability of the caller. Whether the calls include either an artificial voice created by AI or are actually prerecorded by the person whose voice is being used is less important than the requirement that the consumer must have agreed to receive calls using either an artificial or prerecorded voice from that person. The recent action by the FCC against a caller that generated calls pretending to be from President Biden is illustrative of the dangerous misrepresentations these calls can create for recipients.[10] As a result, we recommend that the Commission articulate a rule stating that if a called party has consented to receive calls with an artificial or prerecorded voice from a particular human being, no further

[10] Press Release, Federal Commc'ns Comm'n, FCC Proposes $6 Million Fine for Illegal Robocalls That Used Biden Deepfake Generative AI Voice Message (May 23, 2024), *available at* https://docs.fcc.gov/public/attachments/DOC-402762A1.pdf.

specification about how the calls are created is needed in the consent process, and no disclosure need be provided. However, without that specific prior express consent for calls from a particular person, these calls cannot be legally made.

Recommendation: Informational calls in which a call includes the voice of a particular human being—either artificially created with AI or prerecorded by a particular human being—require the subscriber's prior express consent to receive calls from that particular human being. If there is prior express consent to receive calls from that particular human being, then the in-call disclosure is not required.

3. **Interactive calls.** In these calls, either a) important and/or complex information will be delivered in the call to the recipient (such as information about a debt that the caller claims is owed), or b) more than a simple pressing of a one button is requested of the recipient. Examples include calls from debt collectors, survey calls, and telemarketing calls.

AI-generated debt collection calls have already created a considerable amount of confusion for recipients, many of whom do not understand that they are not talking to a real human being. Whenever interaction is expected between AI and the recipient of the call, it is essential that the recipient must have agreed previously to receive AI-generated calls, and that a disclosure must be provided at the beginning of the call that the caller is using an AI generated voice. Even when calls with AI are made on a limited scale, the degree of confusion and misunderstanding can be considerable. This is illustrated in a recent news article in which a reporter used AI in calls to friends and colleagues.[11]

This is particularly important for debt collection and similar transactional calls. For example, the use of AI is growing quickly among debt collectors. In a 2023 TransUnion survey of debt collection agencies, 11% of respondents reported that they were currently using AI and machine learning (ML)-based technology and an additional 48% were developing or considering the use of such technology.[12] Larger companies have adopted AI/ML at a higher rate than smaller ones thus

[11] Evan Ratliff, *I Created an A.I. Voice Clone to Prank Telemarketers. But the Joke's on Us*., N.Y. Times, Oct. 10, 2024, *available at* https://www.nytimes.com/2024/10/10/opinion/ai-voice-telemarketers.html?smid=nytcore-ios-share&referringSource=articleShare&sgrp=c-cb.

[12] TransUnion, Seizing the Opportunity in Uncertain Times: The Third-Party Collections Industry in 2023, at 39 (2023), *available at* https://www.transunion.com/lp/seizing-the-opportunity-in-uncertain-times-the-collections-indus.

far.[13] Most alarmingly, 53% of the debt collectors currently using or planning to use this technology are using it as "virtual negotiators."[14]

As debt collectors increasingly use digital communications to attempt to reach consumers, they are also harnessing data from those digital channels to decide how to contact consumers in the future. Digital communication platforms "generate valuable data on communication preferences, response times, and engagement patterns."[15] Analytics can be used to personalize the content or tone of a collection communication, the mode of communication, or even the specific debt collector assigned to contact that consumer.[16]

Systems can also learn from engagement with prior communications (*e.g.*, whether the consumer persuaded to make a payment or reveal sensitive information) in order to tailor future messages.[17] Some debt collectors use machine learning to optimize how frequently they communicate, the time of day they communicate, the content and tone of their communications, and the amount of any discount or the length of any payment plan to offer each consumer.[18]

A bipartisan congressional working group on artificial intelligence described how one debt collector is using AI in its text message communications with consumers:

> One panelist described their use of [large language models] to communicate with individuals whose debt is being collected. This panelist uses [generative AI] that produced text prompts, which are then reviewed by a human for legal compliance and sent to customers. These text prompts are refined through engagement analytics and can be tailored to specific collection scenarios. Statistics provided by the panelist indicate a 25 percent increase in payment in full when using AI generated text

---

[13] *Id.* at 40 ("Thirty-six percent of companies with a million or more accounts already use AI/ML-based technology. Adoption by companies servicing less than 100,000 accounts is far lower: Only 4% of these firms actively use it. Fifty-six percent of companies with less than 100,000 accounts have no plans to use AI, versus only 7% of companies with a million accounts or more.").

[14] *Id.* at 39.

[15] FICO, A New Dawn: Modernizing Collections and Recovery in the US 7 (2024), *available at* https://www.fico.com/en/latest-thinking/white-paper/new-dawn-modernizing-collections-and-recovery-us.

[16] Robert J. Szczerba, *Which Industry is Next for A.I. Disruption? The Answer Might Surprise You*, Forbes (updated Jan. 6, 2021), *available at* https://www.forbes.com/sites/robertszczerba/2017/04/26/which-industry-is-next-for-a-i-disruption-the-answer-might-surprise-you/?sh=7356d3a93f1c.

[17] Ryan Lawler, TechCrunch, *Collectly Is Moving Debt Collection Online* (Mar. 28, 2017), *available at* https://techcrunch.com/2017/03/28/collectly-debt-collection/.

[18] Noelle Robillard, TrueAccord, *How TrueAccord Embraces Machine Learning to Create Positive Consumer Experiences in Debt Collection* (Dec. 23, 2021), *available at* https://blog.trueaccord.com/2021/12/how-trueaccord-embraces-machine-learning-to-create-positive-consumer-experiences-in-debt-collections/.

> compared to human generated text. These text prompts are refined through analytics and can be tailored to specific collection scenarios, including if a customer has already accessed their payment portal, how many times they have been communicated with before, and how far along an individual is in the debt collection process.[19]

Using algorithms to generate the settlement terms for a particular consumer may result in disparate treatment of some groups of consumers, some of whom may be offered more favorable repayment terms than other groups.

Voice AI software is increasingly being used to make interactive, live collection calls with consumers.[20] Unless they are informed that the caller is a digital agent, consumers may not know that they are communicating with an AI.[21] The AI may provide consumers incorrect information because of a misunderstanding by the AI of what the consumer was really asking. Even if consumers know that they are speaking to an AI, they may struggle to connect with human agents to discuss complex questions if the debt collector uses the new technology to reduce its staffing of human agents.

Finally, the use of voice AI may significantly increase outbound calls from debt collectors, who will be able to make more calls at a lower cost. One voice AI vendor promises:

> 100% Account Penetration: A Voice AI solution can initiate and handle millions of calls within minutes, covering an agency's entire debt portfolio in an impressively short amount of time. This level of automation has never been possible until recently; it's important to note that over a third of an agency's files often remain untouched.[22]

---

[19] House Committee on Financial Services, Bipartisan Working Group on Artificial Intelligence, Staff Report, AI Innovation Explored: Insights into AI Applications in Financial Services and Housing 17 (July 18, 2024), *available at* https://financialservices.house.gov/uploadedfiles/bipartisan_working_group_on_ai_staff_report.pdf.

[20] TransUnion, Charting the Course and Steering Toward Success: The Collections Industry in 2022, at 29 (Nov. 2022), *available at* https://www.tlo.com/content/dam/tlo/us/documents/dm-22-f108172-3pc-aite-novarica-collections.pdf.

[21] *Compare* Skit.ai recordings without a disclosure (https://skit.ai/?utm_source=ACA_digital&utm_medium=ACA_newsletter&utm_campaign=ACA&utm_id=ACA&ct=t(EMAIL_CAMPAIGN_04_08_2024_COPY_01)) *with* those with a disclosure (https://skit.ai/solution-collection/) (click on embedded videos for call recordings).

[22] Harshad Bajpai, Skit.ai Blog, Entering a New Era of Debt Collections with Conversational Voice AI (Feb. 7, 2023), *available at* https://skit.ai/entering-a-new-era-of-debt-collections-with-voice-ai/.

Making it easier and cheaper to call all the accounts in a debt collector's portfolio has the potential to exponentially increase the number of phone calls to consumers, who may face increased stress and anxiety due to harassment through repeated phone calls.

Recommendation. For these interactive calls, we have three suggestions:

- We fully support the FCC's proposal to require that, before these calls are made, the recipient must have provided prior express consent to receive AI-generated calls after receiving a "clear and conspicuous disclosure" that AI-generated calls would be made.[23] The risks of confusion are sufficiently great to justify this additional layer of assurance that recipients understand they are agreeing to receive calls that use AI. There should be no distinction between calls that use a generic human voice or that of a particular person.

- The disclosure made at the time of consent should also include the commitment that an announcement will be made at the beginning of each consented-to call stating that the call is made with AI-generated technology. In this way, the recipient is actually consenting only to receive AI-generated calls that include the in-call disclosure. If the recipient receives a call that does not include the disclosure, that call will be without consent, and illegal under the TCPA. The disclosure made in every call is especially important for a person who has not consented to receive AI calls, as without it they will not have any way of knowing that the "person" with whom they are conversing is not actually a human being.

  As proposed by the Commission,[24] we support the view that the same rule should apply to all calls that require prior express written consent, including both calls made to lines registered on the Do Not Call list and for telemarketing prerecorded calls made to cell phones and residential lines.[25]

- Finally, and just as importantly, everyone who consents to receive these calls must be able to revoke consent for those calls. That should be explicitly required by an amendment to

[23] AI NPRM, *supra* note 1, at ¶ 14.

[24] *Id.*

[25] We recommend that the Commission cite its authority to protect consumers from these calls in 47 U.S.C. § 227(b)(2) and (c).

the TCPA regulations at 47 C.F.R. § 64.1200(b)(3) to ensure that covered calls include an automated mechanism to opt out of these calls.

II. Protect calls from persons with a disability who use assistive devices to generate the sound of their own words from potential liability under the TCPA.

We fully support the FCC's goal of protecting from potential liability under the TCPA callers with a disability who make calls using assistive technology, including, but not limited to, devices, apps or other software that generate an artificial voice, as proposed in the NPRM.[26] However, we do not believe that it would be wise for this goal to be accomplished by invoking the exemption authority in either of the two statutory provisions, 47 U.S.C. §§ 227(b)(2)(A) and (B), that allow exemptions.

Section 227(b)(2)(B) would allow the Commission to create an exemption for calls to residential lines.[27] Protecting these calls through the FCC's exemption authority is more problematic when the calls are to cell phones. As the FCC recognizes in paragraph 24 of the NPRM, section 227(b)(2)(A) permits the FCC to provide exemptions for calls to cell phones only if the calls are not charged to the called party.[28] The problem is that there are still several prepaid phone plans—those most often used by low-income people—that have limits on the number of minutes for calls. As a result, it is highly unlikely that individuals with disabilities could be sure that all their calls would not be charged to the called party.[29]

Additionally, as the FCC notes in paragraph 27 of its NPRM, using the exemption route would also require the FCC to place a numerical limit on the number of calls that could be made pursuant to the exemption, which would place a compliance burden on the person with a disability using an assistive device to call other people. For these reasons, we are concerned that the

---

[26] AI NPRM, *supra* note 1, at ¶¶ 19-30.

[27] Restrictions on Use of Telephone Equipment, 47 U.S.C. § 227(b)(2)(B) (2024).

[28] 47 U.S.C. § 227(b)(2)(C) (2024).

[29] Tello offers customizable plans in which you can choose limited minutes, starting from 100 minutes per month. The flexibility to adjust minutes and data makes it a popular choice for budget-conscious users. *See* Tello, Build Your Own Plan, *available at* https://tello.com/buy/custom_plans?plan=10GB-unlimited (accessed on Oct. 7, 2024). Tracfone offers low-cost prepaid plans with limited minutes. *See* TracFone, Phone Service Plans, *available at* https://www.tracfone.com/phone-service-plans (accessed on Oct. 7, 2024). Page Plus Cellular, running on Verizon's network, offers a $10 plan that includes 100 minutes of talk. *See* Page Plus Cellular, *available at* https://www.pagepluscellular.com/plans/ (accessed on Oct. 7, 2024).

exemption route will not work to protect calls from persons with disabilities using AI-generated voice in their calls.

But, pursuant to the suggestion made by the FCC to explore alternatives to exemptions, we agree with the FCC's suggestion that the term "artificial voice" can be defined in a way that excludes these calls from all the requirements of the TCPA when callers with disabilities are using assistive technology to communicate by voice over the telephone network.[30]

The voice that is produced by an assistive technology (even when it uses AI) to verbalize the words of a person with a disability over the telephone should not be considered an artificial voice. That voice may be a mechanical voice, because it is mechanically produced, but the fact that it is mechanical does not make it an artificial voice.[31] When the "voice" is the verbalization of the words produced by a person with a disability, that voice is not an artificial voice; it is simply the way that person with a disability vocalizes their words over the telephone. People who do not have a disability use their own voice box to produce the sounds. When a person with a speech disability uses an assistive technology that uses AI to generate speech to express themselves, that is the voice of that person. The device is producing utterances that are the words of the person using the device. That mechanically produced voice may sound a bit different from a voice that is produced by the individual's own body, but the result is just as much the voice of the individual as when the vocalizations are produced by the human's voice box. As a result, the definition of "artificial voice" should exclude a voice that is mechanically produced by an assistive technology, be it a device, app, or other type of software, when used by persons with disabilities who rely on such a device. In this way, these calls would not be covered by the TCPA, and no consent for them would be necessary.

Recommendation. We suggest that the term "artificial voice" as used in the TCPA be defined to exclude a voice mechanically produced by an assistive technology[32] when it is used by a

---

[30] AI NPRM, *supra* note 1, at ¶ 29.

[31] Fabulaa, How can assistive technologies help with communication? https://www.fabulaa.app/how-can-assistive-technologies-help-with- (accessed on Oct. 7, 2024). "High-tech [assistive] devices include speech generation, allowing individuals with impaired speech to make their voices heard. Voice output may be activated by clicking on words or pictures, or typing. New technology uses electromyography (EMG) signals from the brain to control AAC devices for those with paralysis and loss of speech." *Id.*

[32] "The terms *assistive device* or *assistive technology* can refer to any device that helps a person with hearing loss or a voice, speech, or language disorder to communicate. These terms often refer to devices that help a person to hear and understand what is being said more clearly or to express thoughts more easily. With the development of digital and wireless technologies, more and more devices are becoming available to help people with hearing, voice, speech, and language disorders communicate more meaningfully and participate

person with a speech disability who is using such technology to communicate effectively over the telephone.

III. The Commission should prohibit providers from deploying technology that enables network-level, real-time surveillance of the content of calls.

In a Notice of Inquiry included in the same docket,[33] the Commission seeks comment on "the development and availability of technologies on either the device or network level that can: 1) detect incoming calls that are potentially fraudulent and/or AI- generated based on real time analysis of voice call content; 2) alert consumers to the potential that such voice calls are fraudulent and/or AI-generated; and 3) potentially block future voice calls that can be identified as similar AI-generated or otherwise fraudulent voice calls based on analytics."[34] Specifically, the Commission seeks input on whether and how to encourage the development and deployment of these technologies.

These comments, from 26 consumer and privacy advocacy groups and legal aid programs, strongly urge the Commission to prohibit allowing any type of technology that, on a network level, would listen to and/or download or record subscribers' telephone conversations or text exchanges. All the commenting groups have placed a high priority on stopping scam calls and texts, and will continue to urge the FCC to find ways to protect recipients from these dangerous and costly messages. Yet, we are united in strongly opposing any authorization of network-level implementation of these technologies. The threat to the privacy interests in telephone calls and text messages would be so significant that it would severely undermine the value of the nation's telecommunications system.

a. Network-deployed AI technologies will create privacy and security vulnerabilities over which subscribers would have no control.

It is imperative that the Commission do everything in its power to prohibit providers from collecting data about the content of their individuals' communications without the individuals

---

more fully in their daily lives." National Inst. On Deafness and Other Communication Disorders, Assistive Devices for People with Hearing, Voice, Speech, or Language Disorders, What are assistive devices?, *available at* https://www.nidcd.nih.gov/health/assistive-devices-people-hearing-voice-speech-or-language-disorders#:~:text=The%20terms%20assistive%20device%20or,to%20express%20thoughts%20more%20easily.

[33] AI NPRM, *supra* note 1, at IV.

[34] *Id.* at ¶ 35.

providing express, explicit, and affirmative permission to share the content of their calls or texts with anyone, regardless of whether AI is used in that process. While it is important and valuable to incentivize providers to protect consumers from scam calls, this cannot come at the expense of the privacy and data security of the content of individuals' communications.

We strongly support efforts to assist consumers in detecting and avoiding scam calls and texts, but the mechanisms cannot be made applicable at the network level. Doing so would allow impermissible data collection of message content, often without the knowledge of the caller and possibly without the knowledge of the called party, as well. Prohibiting network-level deployment is essential for both data security and data privacy reasons.

The Commission describes these systems as necessarily involving real-time listening to personal calls:

> For example, Google announced it is "testing a new call monitoring feature that will warn users if the person they're talking to is likely attempting to scam them and encourage them to end such calls." This technology will "utilize Gemini Nano — a reduced version of the company's Gemini large language model for Android devices that can run locally and offline — to look for fraudulent language and other conversation patterns typically associated with scams. Users will receive real-time alerts during calls where these red flags are present."[35]

The Commission is right to ask about the privacy implications of deploying real-time scanning of subscriber conversations.[36] One problem is that telecommunications service providers and their vendors are attractive targets for cybercriminals. Within the last several years, each of the three largest carriers has experienced at least one massive breach of subscribers' data (one million or more subscribers impacted).[37] Most recently, this Commission has entered a consent decree with one of the nation's largest voice service providers—AT&T Mobility—because it allowed its vendor to mishandle sensitive customer data.[38]

---

[35] AI NPRM, *supra* note 1, at ¶ 36 (footnotes and citations omitted).

[36] *Id.* at ¶ 40.

[37] *In re* Data Breach Reporting Requirements, Report and Order, Docket No. 22-21, at ¶ 3 n.5 (Rel. Dec. 21, 2023), *available at* https://docs.fcc.gov/public/attachments/FCC-23-111A1.pdf.

[38] Federal Commc'ns Comm'n, *In re* AT&T Services Inc., Order, DA 24-892 (Rel. Sept. 17, 2024), *available at* https://docs.fcc.gov/public/attachments/DA-24-892A1.pdf (consent decree resolving the FCC's "investigation into whether AT&T Services Inc. (AT&T or Company): (i) failed to meet its duty to protect the confidentiality of customer proprietary information (PI); (ii) improperly used, disclosed, or permitted access to individually identifiable customer proprietary network information (CPNI) without customer

Cyberattacks have increased in prevalence[39] and appear to be targeting service providers in the telecommunications system with greater frequency.[40] Allowing systems that use AI to listen to calls to identify patterns that indicate likely scams would present a clear and appealing target for cyberattacks.[41] Because there is never a system that is perfectly secure, integrating one with the nation's telecommunications system—a linchpin of American communications—would create a significant risk to subscribers' personal and sensitive data.[42]

While data security focuses on access unauthorized by the company, data privacy focuses on access unauthorized by the subscriber (even if that access is permitted by the company). Invasions

---

approval; (iii) failed to take reasonable measures to discover and protect against attempts to gain access to CPNI; and (iv) engaged in unjust and unreasonable privacy, cybersecurity, and vendor management practices in connection with a data breach of its vendor's cloud environment that occurred in January 2023") [hereinafter 2024 AT&T Order].

[39] Each year the Federal Bureau of Investigation (FBI) releases an Internet Crime Report that catalogues cybercrime incidents, including personal data breach complaints. In 2023, there were 55,851 complaints related to personal data breaches; this compares with 38,218 complaints in 2019, 27,573 complaints in 2016, and 5,145 complaints in 2014. FBI, 2023 Internet Crime Report 8 (2023), *available at* https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf.; FBI, 2016 Internet Crime Report, 17 (2016), *available at* https://www.ic3.gov/Media/PDF/AnnualReport/2016_IC3Report.pdf.; FBI, 2014 Internet Crime Report 47 (2014), *available at* https://www.ic3.gov/Media/PDF/AnnualReport/2014_IC3Report.pdf. In its 2024 Data Breach Investigation Report (DBIR), Verizon analyzed 30,458 global data breach incidents, with a record high of 10,626 unique data breaches. Verizon Business, 2024 DBIR 5 (2024), *available at* https://www.verizon.com/business/resources/T597/reports/2024-dbir-executive-summary.pdf. An analysis done by the Identify Theft Resource Center (ITRC) found that the number of people affected by data breaches within the first six months of 2024 was more than one billion, a 490% increase from the first half of 2023. ITRC, ITRC H1 Data Breach Analysis: Targeted Cyberattacks Fuel Massive Increase in Breach Victim Counts 6 (2024), *available at* https://www.idtheftcenter.org/publication/itrc-h1-data-breach-analysis/. The ITRC estimates that 2024 had approximately 14% more breaches in the first six months than in the first six months of 2023 (already a record-breaking year), suggesting that 2024 could be even worse. *Id.* at 1.

[40] *See, e.g.*, 2024 AT&T Order, *supra* note 38, at ¶ 2; Stuart E. Madnick, Apple, The Continued Threat to Personal Data: Key Factors Behind the 2023 Increase 2, *available at* https://www.apple.com/newsroom/pdfs/The-Continued-Threat-to-Personal-Data-Key-Factors-Behind-the-2023-Increase.pdf.

[41] *See* Proofpoint, Security Brief: Artificial Sweetener—SugarGh0st RAT Used to Target American Artificial Intelligence Experts (May 16, 2024), *available at* https://www.proofpoint.com/us/blog/threat-insight/security-brief-artificial-sweetener-sugargh0st-rat-used-target-american.

[42] Robert D. Austin & Christopher A.R. Darby, *The Myth of Secure Computing*, Harv. Bus. Rev. (June 2003), *available at* https://hbr.org/2003/06/the-myth-of-secure-computing. *See also* Sarah Krouse, Dustin Volz, Aruna Viswanatha, & Robert McMillan, U.S. Wiretap Systems Targeted in China-Linked Hack, Wall St. J., Oct. 5, 2024, *available at* https://www.wsj.com/tech/cybersecurity/u-s-wiretap-systems-targeted-in-china-linked-hack-327fc63b.

of privacy can result not only in chilling stigmatized behaviors,[43] but also result in emotional[44] and autonomy harms[45] and, in some instances, physical harms.[46]

Some uses of communications services particularly require sensitivity to subscriber privacy—for example, interactions with crisis services like the 988 Suicide and Crisis Lifeline (988 Lifeline).[47] The 988 lifeline not only offers callers a discrete way to discuss their thoughts candidly, but people report using the line because they feel that their information is safe and protected.[48] The perception of confidentiality is critical to enabling people to continue using this service. However, deploying a broad range of AI tools would undermine the incentive for people to use these life-saving services. The feeling of confidentiality in these moments would be eroded by feelings of overt surveillance and caution as to what can be shared candidly in these sensitive situations, especially when stigmas surrounding certain mental health issues are still prevalent and can have a serious impact on one's life.[49] The fact that best practices for these 988 calls is to follow up with a call back to the caller means that—absent guardrails from the Commission—these highly sensitive calls could be listened to, and possibly recorded, subject to real-time call scanning.[50]

Network-originated tools also present threats to the privacy of sensitive calls with health care entities and privileged calls with attorneys. Sensitive health care information is commonly shared by telephone. HIPAA explicitly allows for the transmission of health information in voice calls:[51] health

---

[43] Danielle Keats Citron & Daniel J. Solove, *Privacy Harms,* 102 B.U. L. Rev. 793, 854 (2022).

[44] *Id.* at 841-845.

[45] *Id.* at 845-853.

[46] *Id.* at 831-834.

[47] Substance Abuse and Mental Health Services Administration, 988 Suicide & Crisis Lifeline, *available at* https://www.samhsa.gov/find-help/988 (last visited Oct. 4, 2024).

[48] Christina Caron, *Is the New 988 Suicide Hotline Working?*, N.Y. Times, July 13, 2023, *available at* https://www.nytimes.com/2023/07/13/well/mind/988-suicide-crisis-hotline.html.

[49] Graham Thornicroft et al., *Evidence for effective interventions to reduce mental-health-related stigma and discrimination*, Lancet, 2016 Mar 12;387(10023):1123-1132 (Mar. 2016), *available at* https://pubmed.ncbi.nlm.nih.gov/26410341/.

[50] *See* 988 Suicide & Crisis Lifeline, Crisis Center Guidance: Follow-up with 988 Lifeline Contacts and Those Discharged from Emergency Department and Inpatient Settings 2-5 (updated May 2, 2023), *available at* https://988lifeline.org/wp-content/uploads/2023/07/May-2023-Follow-up-Guidance-Doc.pdf.

[51] U.S. Dep't of Health & Human Servs., Guidance on How the HIPAA Rules Permit Covered Health Care Providers and Health Plans to Use Remote Communication Technologies for Audio-Only Telehealth,

care providers use voice lines to communicate HIPAA-protected information, a patient's appointments test results or specific health care instructions and, at times, they can be used to store patient information itself, like a patient's name and phone number, within a provider's contact book. For the practice of law, this type of surveillance would also undermine a private citizen's confidence about communicating with an attorney by phone.

Instead of considering whether providers and their vendors should create additional repositories of sensitive data, the Commission should consider whether simpler, less privacy-invasive options might be more appropriate to combat scam calls.[52] The current marketplace already offers solutions powered by AI that do not egregiously violate a caller's right to privacy: programs that a user can install on their own device and that can be turned off at any time by the subscriber.[53] While these programs are themselves not without some privacy risks, the risks are substantially less severe than real-time interception of calls controlled at the network level. The Commission should rule that these programs must not be pre-installed on a phone or embedded in upgrades to the device. These programs should be available only if a user, after purchasing the device, specifically opts in to a stand-alone offer that is accompanied by a very plainly worded and prominent description of the program.

b. Real-time call scanning would likely violate multiple existing privacy laws, as the Commission has noted.

We agree with the Commission that scanning the content of communications during a live call may violate federal and state laws.[54] Regardless of the legalities, allowing these technologies on an opt-out basis would pose such significant risks to privacy that it would further erode trust in the

---

available at https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-audio-telehealth/index.html (last visited Oct. 4, 2024).

[52] AI NPRM, *supra* note 1, at ¶ 37 ("Should the Commission act to further the development and deployment of such technologies?").

[53] *See, e.g.*, YouMail, How Does YouMail Actually Work, *available at* https://blog.youmail.com/2013/04/how-does-youmail-actually-work/; YouMail, Features, *available at* https://www.youmail.com/home/features; Robokiller, How It Works (Technology), *available at* https://www.robokiller.com/robocall-blocking-technology; Hiya, How it Works, *available at* https://www.hiya.com/how-it-works (all accessed Oct. 8, 2024). As opposed to live call monitoring, tools like YouMail are set up on a subscriber's phone and direct calls from unknown callers to a voicemail inbox, which forwards a transcription of the message to the subscriber. Tools like those from Hiya and RoboKiller intake metadata about a caller to understand the risk of call spoofing and spam, or may conditionally answer calls for the subscriber for call screening purposes.

[54] AI NPRM, *supra* note 1, at ¶ 40.

nation's telecommunications system. For these reasons, we urge the Commission to deny permission for these proposals to proceed.

At the federal level, the Electronic Communications Privacy Act (ECPA) prohibits the intentional interception of any wire, oral, or electronic communication.[55] The ECPA additionally prohibits the intentional use or intentional attempt to use the contents of any wire, oral, or electronic communication.[56] While there is a distinction in the law between whether the acquisition of communications data occurs during transmission or after the data enters storage, multiple circuit courts have consistently held that information captured in real time (even if it is only accessed later) is considered intercepted communications data, not stored data.[57] Notably, efforts by law enforcement to circumvent these categories have already been stopped dead in its tracks by at least one state court.[58]

There is a private right of action[59] against any person who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication."[60] These remedies may exist even when the complained-of activity was authorized by administrative action.[61] Additionally, even when one party to the communication has consented (for example, when a called party records a communication from a caller), tortious or criminal conduct may still create liability; this could include selling

---

[55] 18 U.S.C. § 2511(1)(a).

[56] 18 U.S.C. § 2511(1)(d).

[57] Luis v. Zang, 833 F.3d 619, 627-31 (6th Cir. 2016) (noting ECPA's distinction between electronic communications and electronic storage, and noting that information captured in real time but viewed later was considered communications subject to Title I of ECPA rather than storage subject to Title II of ECPA); Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 879 (9th Cir. 2002) (same). *See also* U.S. v. Councilman, 418 F.3d 67, 80 (1st Cir. 2005) (messages were electronic communications and were acquired while still en route to intended recipients).

[58] *See, e.g.*, Facebook, Inc. v. State, 296 A.3d 492, 513 (N.J. 2023) (holding that capturing information every fifteen minutes rather than strictly in real time still constitutes a wiretap).

[59] 18 U.S.C. § 2707(a); Rodriguez v. Google L.L.C., 2021 WL 2026726, at *6 (N.D. Cal. 2021).

[60] 18 U.S.C. § 2511(1)(a).

[61] The listed defenses in 18 U.S.C. § 2707(e) do not include authorization by the Federal Communications Commission. Indeed, 18 U.S.C. § 2707(d) contemplates that disciplinary procedures may be brought against federal government employees who improperly authorize illegal activity.

communications data captured as a result of the interception.[62] Additionally, providers might wrongly invoke the "incident to rendition of service" exemption from ECPA regarding call quality.[63] However, call quality monitoring occurs for the purposes of verifying the functional transmission of calls, and is not meant to extend to scanning the content of communications. Moreover, to consider this exception a legal basis for the mass surveillance of subscriber communications allows the exception to swallow the rule and to upend the statute's original intent.[64] As a result, a court reviewing the application of ECPA to these network level tools may find that the ECPA is violated by allowing these systems to operate without specific consent from either the caller or the called party for each call.

While there are exceptions that might mitigate or absolve federal wiretap claims, there is still the matter of state law. Wiretap laws in multiple states would still prohibit this application of AI absent the consent of the caller, as such states require both parties to consent to their communications being recorded.[65] This consent requirement would require clear disclosure to the caller and likely a reminder to the called party who installed the app or service. As with the network

---

[62] *See, e.g.*, Gay v. Garnet Health, 2024 WL 4203263, at *3 (S.D.N.Y. Sept. 16, 2024); M.R. v. Salem Health Hosps. & Clinics, 2024 WL 3970796, at *5 (D. Or. Aug. 28, 2024).

[63] 18 US.C. § 2511(2)(a) (creating an exception explicitly for common carriers and their agents: "any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks"). *See also* Cybertelecom, ECPA: Service Provider Exceptions, *available at* https://cybertelecom.org/security/ecpaisp.htm#net (describing the network operation exception and noting that courts take providers to task for invoking the exception pretextually).

[64] The ECPA was enacted to balance "the privacy expectations of citizens and the legitimate needs of law enforcement." House Committee on the Judiciary, Electronic Communications Privacy Act of 1986, H. Rep. No. 99-647, 99th Cong. 2d Sess. 2, at 19 (1986). Subscribers have a reasonable expectation of privacy in the content of their communications, as the ECPA does not give carriers unconditional access to a subscriber's communications. Although Congress, at the time, recognized that there is an interest in promoting new technologies, these new technologies cannot be expected to succeed if people feel their privacy is not protected. *Id.* This expectation may be diminished where the caller leaves a text or audio message (depending on the details of message playback and storage).

[65] Thompson Reuters, Electronic Surveillance, 0170 SURVEYS 22 (Aug. 2023). These all-party consent states include, but are not limited to, California, Florida, Illinois, Massachusetts, and Pennsylvania.

operation exception to ECPA noted above, state-level exemptions are about the quality of the call itself and not the health of a carrier's call ecosystem as it relates to scam calls.[66]

We applaud the Commission for being willing to explore creative options in combatting scam and otherwise unwanted or illegal calls, but these efforts cannot be at the expense of subscriber privacy, especially not in direct violation of existing wiretap laws. A network-originated AI surveillance tool opens a Pandora's box of privacy and consumer harms, raising concerns not only about the direct interception of a subscriber's call, but also about what happens to the data used on this tool, and who the future stewards of that data will be if these companies are sold or go bankrupt.[67]

[66] In some instances, there is an exception for recording to ensure call quality, and the language parrots the exception of the Wiretap Act (see above), but again, this exception is focused on network mechanics and call quality, not the content of communications nor the features common carriers can offer to subscribers.

[67] *See* Erin Griffith, *From Unicorns to Zombies: Tech Start-Ups Run Out of Time and Money*, N.Y. Times, Dec. 7, 2023, *available at* https://www.nytimes.com/2023/12/07/technology/tech-startups-collapse.html; Matt Reynolds, Wired, *If you can't build it, buy it: Google's biggest acquisitions mapped* (Nov. 25, 2017), *available at* https://www.wired.com/story/google-acquisitions-data-visualisation-infoporn-waze-youtube-android (it is a reality of the modern technology companies that it is easier for companies to purchase them than to compete with them).

IV. Conclusion

We appreciate the Commission's consideration of our proposals and concerns. We would be happy to answer any questions.

Submitted October 10, 1953, by:

Margot Saunders
Carolyn Carter
National Consumer Law Center
On behalf of its low-income clients
1001 Connecticut Ave, NW
Washington, DC 20036
msaunders@nclc.org

Chris Frascella
Matthew Contursi
Electronic Privacy Information Center
1519 New Hampshire Ave, NW
Washington, DC 20036
frascella@epic.org

Appendix

National Groups

For over 50 years, the **National Consumer Law Center** (NCLC) has played a leading role in crafting the laws and regulations that protect consumers from abusive and deceptive transactions. NCLC uses its proficiency in consumer law to protect consumers from exploitation and expand access to fair credit by advocating for laws, rules, and regulations that benefit real people: those with low incomes, older people, students, people of color, and others who have been abused, deceived, discriminated against, or left behind in our economy. NCLC is at the center of a national network of legal aid lawyers, private attorneys, elder advocates, housing counselors, pro-consumer policymakers and enforcement officials, and other allies who use NCLC's expertise to fight for consumers on the front lines, day in and day out. www.nclc.org

Consumer Action has been a champion of underrepresented consumers since 1971. A national, nonprofit 501(c)3 organization, Consumer Action focuses on financial education that empowers low to moderate income and limited-English-speaking consumers to financially prosper. It also advocates for consumers in the media, and before lawmakers and regulators, to advance consumer rights and promote industry-wide change particularly in the fields of credit, banking, housing, healthcare, privacy, insurance and telecommunications. www.consumer-action.org

Consumer Federation of America (CFA) is a national association of over 250 nonprofit organizations that advances the consumer interest through research, advocacy, education, and service. CFA investigates consumer issues and publishes research that assists policymakers and individuals, and it has worked to end the scourge of unwanted calls and texts that plague consumers and jeopardize our national communications infrastructure. https://consumerfed.org/

The **Electronic Privacy Information Center** (EPIC) is a public interest research center in Washington, DC seeking to protect privacy, freedom of expression, and democratic values in the information age. https://epic.org/

The **National Association of Consumer Advocates** (NACA) is a non-profit organization with a membership of private and public sector attorneys, legal services attorneys, law professors, and law students whose primary interest is the protection and representation of consumers. NACA's mission is to promote justice for all consumers by maintaining a forum for information sharing among consumer advocates across the country and to serve as a voice for its members and consumers in the ongoing struggle to curb unfair, deceptive, and abusive business practices. https://www.consumeradvocates.org/

The **National Consumers League** is a non-profit, non-partisan consumer advocacy organization representing consumers and workers on marketplace and workplace issues since its founding in 1899. Headquartered in the District of Columbia, NCL provides government, businesses, and other organizations with the consumer's perspective on concerns including child labor, privacy, food safety, telecommunications, and medication information. https://nclnet.org/

Public Knowledge is a non-partisan, non-profit consumer rights organization dedicated to promoting freedom of expression, an open internet, and access to affordable communications tools and creative works. It has worked for many years to promote telecommunications policies that protect consumers, and has filed comments to the Federal Communications Commission (FCC) on

proposals supporting the protections of the Telephone Consumer Protection Act (TCPA) and the practical, effective, and balanced regulation of AI. https://publicknowledge.org

U.S. Public Interest Research Group, a non-partisan, non-profit organization founded more than 50 years ago, focuses on problems that affect the public's health, safety and financial well-being. https://pirg.org/

State and Local Groups

Bay Area Legal Aid serves low-income consumers as the largest provider of civil legal aid across seven San Francisco Bay Area counties. https://baylegal.org/

Established in 1937, **Jacksonville Area Legal Aid** is a nonprofit law firm in **Florida** focused on delivering economic, social, and housing justice to low-income and at-risk individuals and families on the First Coast. https://www.jaxlegalaid.org/

Idaho Legal Aid Services is a not-for-profit civil legal services provider for the state of Idaho serving low-income Idahoans. https://www.idaholegalaid.org/

Indiana Legal Services, Inc., is a nonprofit law firm that provides free civil legal assistance to eligible low-income residents throughout the state of Indiana. https://www.indianalegalservices.org/

Mid Minnesota Legal Aid provides free legal aid to residents of 20 Minnesota Counties. https://mylegalaid.org/

Legal Aid of Western Missouri provides free civil legal services to low-income and vulnerable individuals in 40 counties in Missouri. https://lawmo.org/

Montana Legal Services (MLSA) is a private, non-profit law firm that provides non-criminal legal information, advice, and representation to thousands of Montanans each year. https://www.mtlsa.org/

Legal Aid of Nebraska is a not-for-profit civil legal services provider for the state of Nebraska serving low-income Nebraskans. www.LegalAidOfNebraska.org

603 Legal Aid is **New Hampshire's** LSC-funded non-profit legal service organization, providing legal services to Granite Staters living with low-income. https://www.603legalaid.org/

Established in 1993, **CAMBA Legal Services** of **New York** provides free legal counsel and representation to over 12,000 low-income New Yorkers each year in the areas of Housing Law, Foreclosure Prevention, Domestic Violence, Consumer Law, Public Benefits, and Immigration Law. CAMBA.org

The **Western New York Law Center, Inc**. (WNYLC) is a nonprofit legal services provider headquartered in Buffalo, NY that provides services throughout Western New York. Founded in 1996, WNYLC's mission is to promote human and civil rights guided by an overarching commitment to racial and economic justice. WNYLC works to ensure that low-income people have

fair and equitable housing, credit, and community economic development by providing legal services including individual representation in housing, consumer debt, and other matters, as well as "non-traditional" legal assistance in the form of policy advocacy, community legal education, and impact litigation to address systemic issues. https://wnylc.com/

The **North Carolina Justice Center** (NCJC) champions the rights of North Carolinians with low incomes by addressing the systemic inequities at the root of economic injustice. NCJC's mission is to eliminate poverty in North Carolina by ensuring that every household in the state has access to the resources, services, and fair treatment it needs to achieve economic security. https://www.ncjustice.org/

The **Pennsylvania Utility Law Project** (PULP) is a statewide specialty legal services project of Regional Housing Legal Services and is a member of the Pennsylvania Legal Aid Network. Our mission is to secure just and equitable access to safe and affordable utility services for Pennsylvanians experiencing poverty. PULP works to achieve this mission through representation, advocacy, education, and support services to individuals and community groups. https://www.pautilitylawproject.org/

Community Legal Services of Philadelphia ("CLS") provides free civil legal assistance to low-income Philadelphians when they face the threat of losing their homes, incomes, health care and even their families. CLS provides a full range of legal services, from individual representation to administrative advocacy to class action litigation, as well as community education and social work. Since its founding in 1966, CLS has served more than one million low-income Philadelphians. https://clsphila.org/

Legal Aid Services of Oklahoma (LASO) is the Oklahoma statewide provider of civil legal services to low-income persons. www.legalaidok.org

The **Legal Aid Justice Center** (LAJC) of **Virginia** partners with communities and clients to achieve justice by dismantling systems that create and perpetuate poverty. LAJC provides legal advice and direct legal representation each year to thousands of low-income individuals who cannot afford private counsel in civil practice areas such as consumer protection, landlord-tenant, employment, immigration, and civil rights. https://www.justice4all.org/contact/

Mountain State Justice is a non-profit legal services and advocacy organization representing low-income **West Virginians**. Since our founding in 1996, we have represented thousands of consumers, including in debt collection defense matters. https://mountainstatejustice.org/

The mission of **Legal Action of Wisconsin** is to deliver exceptional civil legal services and structural change advocacy, free of cost, to those most in need. https://legalaction.org/