2024 Report of the Federal Communications Commission Consumer Advisory Committee

I. Summary

The Federal Communications Commission's ("FCC" or "Commission") Consumer Advisory Committee ("CAC") is pleased to submit the following report and recommendations to the FCC examining the uses of artificial intelligence ("AI") to protect consumers from unwanted robocalls, robotexts, and other harms, and to enable people with disabilities to make calls. Over the past six months, the CAC met three times as a full committee and multiple times in working groups to develop this report. The CAC drew on the expertise of its members as well as outside experts in artificial intelligence, enforcement, and disability access to develop the following recommendations.

In total, this report provides the Commission with sixteen individual recommendations. These include recommendations for greater coordination with other agencies on comprehensive solutions to protect consumers from the use of AI for malicious calling purposes, promoting innovative uses of AI to enhance call-blocking technologies, and consideration of the privacy risks associated with the use of AI-based robocall identification and blocking tools. Regarding outreach and education, the CAC's recommendations include a national public education and engagement effort to empower consumers to recognize, react, and report appropriately and safely when an unwanted or malicious robocall or robotext is received. The report also includes a recommendation that the Commission integrates an AI robocall and robotext education campaign along with broadband access and literacy initiatives.

"The anxiety about these technology developments is real. Rightfully so. But I think we make a mistake if we only focus on the potential for harm. We need to equally focus on how artificial intelligence can radically improve the tools we have today to block unwanted robocalls and robotexts. We are talking about technology that can see patterns in our network traffic unlike anything we have today. This can lead to the development of analytic tools that are exponentially better at finding fraud before it ever reaches us at home. Used at scale, we can not only stop this junk, we can help restore trust in our networks."

- FCC Chairwoman Jessica Rosenworcel (November 15, 2023)

II. Background

As Chairwoman Rosenworcel has recognized, AI promises great potential for consumers, including in the fight against malicious calling.¹ At a time of already-rising fraud,² however, AI also presents substantial risks to consumers as bad actors use AI for malicious purposes.

On March 28, 2024, FCC Chairwoman Jessica Rosenworcel tasked the twelfth term of the FCC's CAC with examining the uses of AI, how it might protect consumers from unwanted robocalls, robotexts, and other harms, and how it may enable individuals with disabilities to make calls. Specifically, the Chairwoman charged the Committee to produce a report that includes findings on:

- 1. How the Commission can help prevent AI from being used for malicious calling purposes
- 2. How AI is being used to help consumers avoid unwanted robocalls and robotexts
- 3. How the Commission can encourage such uses
- 4. How AI is being used to enable people with disabilities to make calls
- 5. How the Commission can encourage those uses consistent with the requirements of the Telephone Consumer Protection Act and ensure its future anti-robocall work does not deter them
- 6. What outreach or education should be conducted in order to keep consumers informed about the development of these technologies and applications

III. Definitions

"Artificial intelligence" encompasses a wide range of technologies and functions and has been defined by a variety of organizations in different ways.

15 U.S. Code § 9401 defines artificial intelligence as a "machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments. Artificial intelligence systems use machine and human-based inputs to— A) perceive real and virtual environments; B) abstract such perceptions into models through analysis in an automated manner; and c) use model inference to formulate options for information or action."

¹ "From my perch as the head of our Nation's expert agency on communications, I can't help but be an optimist about the future of AI." "Remarks of FCC Chairwoman Jessica Rosenworcel Federal Communications Commission and National Science Foundation Joint Workshop," *Federal Communications* Commission, July 13, 2023. ("From my perch as the head of our Nation's expert agency on communications, I can't help but be an optimist about the future of AI."); <u>https://docs.fcc.gov/public/attachments/FCC-23-101A2.pdf</u> ("We need to equally focus on how artificial ;

[&]quot;We need to equally focus on how artificial intelligence can radically improve the tools we have today to block unwanted robocalls and robotexts. We are talking about technology that can see patterns in our network traffic unlike anything we have today. This can lead to the development of analytic tools that are exponentially better at finding fraud before it ever reaches us at home. Used at scale, we can not only stop this junk, we can help restore trust in our networks." "Statement of Chairwoman Jessica Rosenworcel re: Implications of Artificial Intelligence Technologies on Protecting Consumers from Unwanted Robocalls and Robotexts," *Federal Communications* Commission, November 15, 2023. <u>https://docs.fcc.gov/public/attachments/FCC-23-101A2.pdf</u>

² "As Nationwide Fraud Losses Top \$10 Billion in 2023, FTC Steps Up Efforts to Protect the Public," *Federal Trade* Commission, February 9, 2023. <u>https://www.ftc.gov/news-events/news/press-releases/2024/02/nationwide-fraud-losses-top-10-billion-2023-ftc-steps-efforts-protect-public</u>

The Commission has proposed to define an AI-generated call or text as "a call that uses any technology or tool to artificially generate a voice or 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."³

This report will use the definitions above. The CAC takes no position on the merits of these definitions.

IV. Findings

1. How can the Commission help prevent AI from being used for malicious calling purposes?

Consistent with the CAC's charge, this report focuses on the use of AI for "malicious calling purposes." For purposes of this report, the CAC's interpretation of "malicious calling purposes" is informed by the Telephone Consumer Protection Act ("TCPA") and Truth in Caller ID Act. Among other things, the TCPA requires prior express consent for a caller to make a call using an automatic telephone dialing system or prerecorded or artificial voice to a consumer.⁴ The FCC recently clarified that a call made using an AI-generated voice is an "artificial voice" for purposes of the TCPA,⁵ and more recently has sought comment on defining an "AI-generated voice."⁶ The Truth in Caller ID Act makes it unlawful to transmit misleading or inaccurate caller identification ("caller ID") information (i.e., "spoofing") with the intent to defraud, cause harm, or wrongfully obtain anything of value."⁷ The CAC's recommendations can apply to AI-generated calls that violate either or both of these statutes.

RECOMMENDATION #1: The FCC should partner with other federal agencies and the White House to ensure that there is a comprehensive solution across all agencies that helps prevent AI from being used for malicious calling purposes.

Using the aforementioned laws as guidance, this report considers "malicious calling activities" to be calling activities that violate the TCPA (e.g., unsolicited robocalls or robotexts), as well as spoofed calls intended to defraud, cause harm, or wrongfully obtain anything of value from the consumer. Fraud calls made using AI may, for instance, violate both the TCPA and the Truth in Caller ID Act, as well as other statutes (e.g., criminal fraud laws).

³ "Implications of Artificial Intelligence Technologies on Protecting Consumers from unwanted Robocalls and Robotexts," *Federal Communications Commission*, July 17, 2024.

https://docs.fcc.gov/public/attachments/DOC-404036A1.pdf

⁴ 47 USC 227(b)(1). <u>https://www.law.cornell.edu/uscode/text/47/227</u>

⁵ "In the Matter of Implications of Artificial Intelligence Technologies on Protecting Consumers from Unwanted Robocalls and Robotexts," *Federal Communications Commission*, February 8, 2024. https://docs.fcc.gov/public/attachments/FCC-24-17A1.pdf

⁶ "Implications of Artificial Intelligence Technologies on Protecting Consumers from Unwanted Robocalls and Robotexts," *Federal Communications Commission*, July 17, 2024. <u>https://docs.fcc.gov/public/attachments/DOC-404036A1.pdf</u>;

[&]quot;FCC Launches Inquiry into AI's Impact on Robocalls and Robotexts," *Federal Communications Commission*, August 28, 2024. <u>https://www.fcc.gov/consumer-governmental-affairs/fcc-launches-inquiry-ais-impact-robocalls-and-robotexts</u>

⁷ "Truth in Caller ID Act of 2009," *Library of Congress*, December 22, 2010. https://www.congress.gov/111/plaws/publ331/PLAW-111publ331.pdf

Note: For purposes of brevity, when this report refers to "robocalls," it is referring to both robocalls and robotexts, unless otherwise noted. This is consistent with the Commission's 2015 TCPA Omnibus Declaratory Ruling and Order ("In this Declaratory Ruling and Order, we refer to calls that require consumer consent under the TCPA as 'robocalls,' 'covered calls and texts,' or 'voice calls and texts.'").⁸

Malicious calling examples historically can be divided into at least two key types. First, malicious calling can be (i) high-volume, where the bad actor randomly calls as many individuals as possible, or (ii) targeted, where the bad actor calls specific known individuals.⁹ Second, malicious calling can be (i) illegal telemarketing that violates the TCPA and other telemarketing laws and where some real product or service is sold,¹⁰ or (ii) outright criminal fraud where the bad actor seeks to use a pretense to either directly access an individual's financial accounts or have such person send funds to them.¹¹

While bad actors' use of AI for malicious calling purposes is still nascent, there is every reason to believe bad actors will use AI for all of the malicious calling activities described above. And although there is limited concrete public evidence and data available regarding how they are using AI and at what scale, AI technologies may present the following capabilities to bad actors as part of their malicious calling efforts:

• *Targeted AI Voice Cloning for Fraud.* Voice cloning – the capability to generate a near-perfect voice clone based on a short audio clip or snippet of someone's voice – offers tremendous potential to help people, including individuals with disabilities as described below. However, as the FTC has noted "in the wrong hands, voice cloning technologies can do harm. Take, for example, the family emergency scam, where an impostor pretends to be a distressed relative. A scammer could clone a voice that sounds just like your loved one. Scammers could also clone the voice of a CEO or other company executive and then trick employees into transferring large sums of money or to pay a fake invoice."¹²

⁸ "In the Matter of Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991," *Federal Communications Commission*, July 10, 2015. <u>https://docs.fcc.gov/public/attachments/FCC-15-72A1.pdf</u>

 ⁹ "Prepared Testimony of Joshua M. Bercu...Hearing on Protecting Americans from Robocalls," U.S. Senate Committee on Commerce, Science, & Transportation Subcommittee on Communications, Media and Broadband, October 24, 2023. <u>https://www.commerce.senate.gov/services/files/9E0BFE0C-E920-4C89-BE35-B2A4A8396181</u>;
 "Re: Enforcement Bureau Requests Information on the Status of Private-Led Traceback Efforts of Suspected Unlawful Robocalls," *Federal Communications Commission*, November 13, 2023. <u>https://www.fcc.gov/ecfs/document/11130588416636/1</u>

¹⁰ "FCC Closes TCPA Lead Generator Loophole; Requires One-to-One Consent," *Orrick*, December 20, 2023. <u>https://www.orrick.com/en/Insights/2023/12/FCC-Closes-TCPA-Lead-Generator-Loophole-Requires-One-to-One-Consent</u>

¹¹ "Prepared Testimony of Joshua M. Bercu...Hearing on Protecting Americans from Robocalls," U.S. Senate Committee on Commerce, Science, & Transportation Subcommittee on Communications, Media and Broadband, October 24, 2023. <u>https://www.commerce.senate.gov/services/files/9E0BFE0C-E920-4C89-BE35-B2A4A8396181</u>;

[&]quot;Re: Enforcement Bureau Requests Information on the Status of Private-Led Traceback Efforts of Suspected Unlawful Robocalls," *Federal Communications Commission*, November 13, 2023. https://www.fcc.gov/ecfs/document/11130588416636/1

¹² "Announcing the FTC's Voice Cloning Challenge," *Federal Trade Commission*, November 16, 2023. https://consumer.ftc.gov/consumer-alerts/2023/11/announcing-ftcs-voice-cloning-challenge

- *High-Volume Voice Cloning for Fraud or Other Malicious Purposes.* The Commission recently addressed allegations involving robocalls purportedly containing an AI-generated deepfake audio recording of President Biden's voice telling prospective voters not to vote in advance of New Hampshire's 2024 presidential primary election.¹³
- *Increasing Scale Historically Targeted Malicious Calling.* For purposes of targeted fraud or targeted illegal telemarketing, AI can allow bad actors to scale what would otherwise be more limited calling activities. Historically, these type of targeted calls and texts have involved a live caller or message sender (or a live operator using a soundboard) to react to the called party as naturally as possible. AI calling and texting can allow bad actors to broaden these targeted, seemingly natural conversations.
- *Improving Quality of Scams.* AI can help bad actors improve the quality of their scams, whether through AI voice cloning or more simply by improving calling or texting scripts. For example, AI may enable criminals whose native language is not English to improve their pitches by eliminating common grammatical mistakes that tip off English speakers that a message sender may not be American.

RECOMMENDATION #2: The CAC recommends that the FCC explicitly declare that a call made with an AI-generated voice with the intent to defraud, harm, or deceive the recipient always violates the TCPA, as no reasonable consumer would knowingly consent to such a call made with an artificial voice.

Regarding voice cloning, the FCC has already taken a significant step to address this threat: namely, the February 8, 2024 Declaratory Ruling that confirmed that the TCPA's restrictions on the use of "artificial or prerecorded voice" encompass current AI technologies that generate human voices, such as voice cloning technologies, and therefore require the prior express consent of the called party to initiate such calls absent an emergency purpose or exemption.¹⁴ Robust enforcement of the Commission's illegal robocall rules including the TCPA, additional blocking and forfeiture mechanisms that the Commission intends to adopt in September 2024, collaboration with state attorneys general to increase resources and enforcement capabilities, and utilization of consumer complaint data shared by the Federal Trade Commission ("FTC") would aid this effort. Additionally, increasing fines for fraud could also be a deterrent. We recommend that the FCC consider additional ways to support voice service providers' work to identify and block these illegal calls.

¹³ "FCC proposes \$6 million fine for illegal robocalls that use Biden deepfake generative AI voice message,"
 Federal Communications Commission. May 23, 2024. <u>https://docs.fcc.gov/public/attachments/DOC-402762A1.pdf</u>
 ¹⁴ "In the Matter of Implications of Artificial Intelligence Technologies on Protecting Consumers from Unwanted Robocalls and Robotexts," *Federal Communications Commission*, February 8, 2024. https://docs.fcc.gov/public/attachments/DOC-402762A1.pdf

Additionally, the FCC has initiated a proposed rulemaking to apply TCPA restrictions to AI-generated robocalls and robotexts¹⁵ as well as a Notice of Inquiry to gather additional information about the tools that are being developed and how those tools can be introduced into the ecosystem.¹⁶

The CAC looks forward to seeing how the record develops as the Commission considers whether to require callers, when obtaining prior express consent, to disclose to the recipient that the caller intends to use AI-generated calls and text messages, and whether to require that some AI-generated calls must include a disclosure during the call. The CAC further welcomes the Commission's consideration of how the TCPA and other restrictions apply to these technologies and which uses should be exempted. The CAC also welcomes the Commission's effort to ensure that individuals with disabilities can use AI technologies without obtaining prior express consent from the recipient of their calls.

Efforts by agencies to promote the development of such tools have achieved notable results. For example, the Federal Trade Commission's Voice Cloning Challenge awarded prize money to entities that developed products, policies, and procedures aimed at protecting consumers from AI-enabled voice cloning harms. The FTC's challenge aimed to foster breakthrough ideas on preventing, monitoring, and evaluating malicious voice cloning.¹⁷

RECOMMENDATION #3: The CAC recommends that the Commission consider launching, potentially on an expedited basis, a workshop, showcase, or other initiative to encourage voice service providers, analytics providers, and other stakeholders to develop, demonstrate and implement AI detection and mitigation technologies to block calls identified as likely to contain AI voice cloning.

2. How is AI being used to help consumers avoid unwanted robocalls and robotexts?

Over the last decade, in conjunction with FCC and other government action, communications providers have deployed numerous tools to protect consumers from illegal and unwanted robocalls and robotexts. These include:

- Blocking and labeling analytics, made available at no charge to either block calls outright or give consumers information about a call to inform their decision to answer the call;
- Network-level blocking;
- The STIR/SHAKEN caller ID authentication framework;
- Know-your-customer ("KYC") and know-your-upstream-provider ("KYP") efforts; and
- Industry traceback

¹⁵ "Implications of Artificial Intelligence Technologies on Protecting Consumers from Unwanted Robocalls and Robotexts," *Federal Communications Commission*, July 17, 2024. <u>https://docs.fcc.gov/public/attachments/DOC-404036A1.pdf</u>

¹⁶ "FCC Launches Inquiry into AI's Impact on Robocalls and Robotexts," *Federal Communications Commission*, August 28, 2024. <u>https://www.fcc.gov/consumer-governmental-affairs/fcc-launches-inquiry-ais-impact-robocalls-and-robotexts</u>

¹⁷ "The FTC Voice Cloning Challenge," *Federal Trade Commission*. <u>https://www.ftc.gov/news-events/contests/ftc-voice-cloning-challenge</u>

In addition to those offered by communications providers, over-the-top apps offer additional options for customers. For example, robocall blocking service YouMail uses AI to identify unwanted scam and telemarketing calls and texts. It can then block these messages for its own retail customers. But, of even more importance: YouMail works with different actors along the call and text pathways to notify them of these unwanted calls and texts so they can be blocked for all recipients. YouMail's AI-driven system analyzes patterns and behaviors associated with spam and fraudulent calls, using machine learning algorithms to identify and filter out these unwanted communications more effectively.

In many cases, blocking and labeling analytics are powered by machine learning, a form of automation that is not generative AI. While generative AI is a powerful tool, it is not necessarily the best solution for every problem. For example, the CAC received feedback from an expert on the use of AI by voice service providers that providers may also utilize machine learning and other automation, such as discriminative AI, as part of their network blocking, and KYC and KYP processes.¹⁸

Most of the currently-deployed industry robocall and robotext mitigation tools are technology agnostic and are intended to identify and stop malicious calls and texts, regardless of whether the originators of such calls or texts used AI to produce the calls or texts. Provider-deployed blocking and labeling analytics, for instance, detect suspicious calling patterns and take action when such patterns are identified, without relying on call content, since providers cannot listen to the content of all calls either legally or technically. These tools can effectively protect consumers against AI-generated malicious calling activities since they can still identify suspicious patterns, such as high-volume AI calling and texting, and their use should be encouraged.

Likewise, service providers take steps to vet their customers and upstream voice service providers, which helps to reduce malicious traffic on their networks, regardless of whether such traffic is AI-generated or not. Finally, service providers are obligated to cooperate with the Industry Traceback Group ("ITG"), which identifies the entities responsible for illegal calls, regardless of whether such calls are spoofed. In 2024, the ITG traced back an illegal robocall campaign that cloned President Joe Biden's voice, which helped lead to FCC enforcement against the calling party and provider responsible for originating the calls.¹⁹

New and emerging technologies are focused on identifying synthetic voices and/or watermarking lawfully cloned voices. Last year, the FTC launched a voice cloning challenge to identify tools that can help identify maliciously cloned voices. Winning submissions proposed useful tools to detect synthetic voices that utilize AI algorithms to detect the subtle differences between genuine and synthetic voice patterns, forms of watermarking to make it more difficult to clone accurately, and a technique that authenticates the human origin of voice recordings when created and then embeds this authentication as a watermark or signature in the stream. The runner up has developed a technology that detects voice clones and deep fakes in real time.²⁰

As the government continues to encourage the development and use of AI tools to mitigate fraudulent

¹⁸ Presentation by Greg Bohl, Chief Data Officer of Transaction Network Services, to the FCC Consumer Advisory Committee. June 7, 2024.

 ¹⁹ "FCC Proposes \$6 Million Fine for Illegal Robocalls That Used Biden Deepfake Generative AI Voice Message," *Federal Communications Commission*, May 23, 2024. <u>https://docs.fcc.gov/public/attachments/DOC-402762A1.pdf</u>
 ²⁰ "The FTC Voice Cloning Challenge," *Federal Trade Commission*. <u>https://www.ftc.gov/news-events/news/press-releases/2024/04/ftc-announces-winners-voice-cloning-challenge</u>

communications, the CAC also urges the Commission to consider how AI tools can be used to serve the dual purpose of reducing incidents of false positives and blocking or mislabeling of legitimate traffic.

RECOMMENDATION #4: The CAC recommends that the Commission continue to support voice service providers' deployment of current and additional tools and processes to identify, block, label (as appropriate), and otherwise mitigate illegal and unwanted calls and texts, including any such calls and texts that are AI-generated, while ensuring appropriate redress mechanisms for legitimate callers.

In addition, in its NPRM released August 8, 2024, the FCC notes new tools in development:

The record highlights several examples of call detection and alerting technologies that can help detect scam calls or calls that use AI-generated voice based on real time content analysis of the incoming call. 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." Other technologies under development seek to authenticate human voice as a method of thwarting calls featuring AI-generated voices, such as scam calls that do not disclose the use of AI."

Other tools cited by the Commission include:

"Microsoft's Azure Operator Call Protection is a data based service offered to telephone service providers at the network level that "detects potential phone scams, performs real-time AI-driven analysis of consumer phone calls, and alerts subscribers when they are at risk of being scammed."

RECOMMENDATION #5: The CAC recommends that the Commission consider how risks to privacy and compliance with privacy laws may be impacted by the use of call detection and alerting technologies that monitor the content of calls made to consumers while the Commission evaluates the potential benefits of these technologies in combating unwanted spam and fraudulent calls.

3. How can the Commission encourage such uses?

As discussed above, AI technologies are still emerging and the use of AI by bad actors is undergoing rapid change. The Commission must stay abreast of these changes to best protect consumers.

RECOMMENDATION #6: The CAC recommends that the Commission consider periodically seeking comment on the state of the AI-generated robocall and robotext threat environment and the technologies being used or developed to address these threats.

RECOMMENDATION #7: The CAC recommends that the Commission encourage collaboration among voice service providers, app developers, handset manufacturers and other relevant participants to develop tools that can help identify and combat AI used for malicious calling purposes.

To the extent entities develop tools that enable monitoring and analysis of call content to detect scams or malicious calling practices, the Commission should encourage these entities to consider how best to provide transparency and control for consumers while mitigating privacy risks.

RECOMMENDATION #8: The CAC recommends that the Commission task a future advisory committee (that includes representatives of consumers) with developing a report that would examine specific topics related to the implementation of AI by industry stakeholders and other relevant participants to help consumers avoid unwanted robocalls and robotexts. Such topics could include consumer notice; whether consumers can opt-in or must opt-out of the AI detection tools; mechanisms for consumer feedback; consumer adjustment of tools to ensure receipt of legitimate calls and texts; evaluate the privacy implications of any data collection and retention used by the tools; customer control of data collection; and cost to consumers.

4. How is AI being used to enable people with disabilities to make calls?

A growing number of AI technologies are used to enable people with disabilities to make calls. Examples include:

- AI products that allow individuals with mobility disabilities to place calls through voice commands, a feature available on most smartphones. Modern AI products can also better detect and adapt to non-standard speech, expanding the availability to voice-command functions.
- AI services that can enhance detection of non-verbal motions, like eye movements and American Sign Language, allowing these movements to control digital interfaces and place calls.
- Text-to-speech voice-modeling software that can enable individuals with limited speaking capabilities to have a verbal conversation, with some products able to model an individual's speaking voice. Anti-spam measures that rely on artificial voice detection should allow these conversations.
- AI tools can act as a voice for someone who cannot speak, either due to a speech disability or due to a debilitating disease. This not only helps the individual carry out everyday tasks and can increase their employment opportunities.

5. How can the Commission encourage those uses consistent with the requirements of the Telephone Consumer Protection Act and ensure its future anti-robocall work does not deter them?

Just as the Commission can encourage the uses of AI to help consumers avoid unwanted telecommunications, the FCC can create exemptions that encompass expressly approved uses of AI to help individuals with disabilities make calls and outline best practices for these service-providers. 47 U.S.C. § 227(b)(2)(B), (C) provides this authority to the Commission.

RECOMMENDATION #9: The CAC recommends the Commission take all steps within its authority to ensure that its robocall regulations do not deter development and use of AI-powered tools that enable people with disabilities to better use the telephone network. We welcome the Commission's consideration of whether existing law allows it to exempt such uses from the TCPA and whether changes to the law may be necessary. Additionally, we recommend that the Commission ensure that these exemptions cannot be exploited by bad actors.

Additionally, the FCC should regularly hear from individuals with disabilities who use AI-assistive technology and the developers of such tools to ensure that the Commission's critical enforcement activities do not unintentionally hamper these tools. Social media and other web postings should solicit this feedback, but the FCC should proactively attempt to reach these individuals and developers as well.

6. What outreach or education should be conducted in order to keep consumers informed about the development of these technologies and applications?

To promote consumer awareness and trust in compliant AI services, the FCC should create a <u>website with</u> <u>potential AI tools</u> and take the steps mentioned in Sections 1-3 of this report. Specifically, the website should provide educational materials regarding AI-enabled services that can 1) help consumers avoid unwanted robocalls and robotexts and/or 2) help individuals with disabilities to make calls and/or texts. This registry should be hosted online, publicly accessible, and easily understandable.

The following section outlines recommendations for a national consumer education and engagement campaign that places intentional focus on community-level outreach strategies and partnerships the Commission can leverage to maximize the reach and efficacy of this campaign. The CAC believes operationalization of these recommendations can advance the goal of preparing and protecting **all** consumers when it comes to AI-generated robocalls and robotexts.

RECOMMENDATION #10: The CAC recommends that the Commission develop national public education and engagement efforts based on a "3R" Response to empower consumers to recognize, react, and report appropriately and safely when an unwanted or malicious robocall or robotext is received.

The Committee recommends that the Commission engage in a public education campaign to help consumers understand when robocalls and robotexts received are generated by AI. This campaign should inform consumers, at least at a basic level, of what AI is and provide examples of common use cases for AI-powered tools. A campaign should also explain the available call blocking tools or Commission-approved phone applications that may be installed to detect and prevent AI-driven robocalls and robotexts.

This public campaign could follow a two-pronged approach. The first aim is to educate consumers on the emerging uses of AI-generated technologies impacting robocalls and robotexts and related telecommunications issues. Second, the campaign could educate consumers on the risks and harmful impacts of scams and fraud posed by AI-generated robocalls and robotexts.

Additionally, acknowledging that not all AI-generated calls and texts are harmful and, in fact, can be beneficial, particularly for people with certain disabilities, an education campaign should highlight the affirmative use cases of AI related to telecommunications services. To better understand and catalog those affirmative telecommunications use cases for AI, the Commission should consult vulnerable groups, disability groups, other federal agencies with intersectional expertise, and technologists.

RECOMMENDATION #11: The CAC recommends that the Commission develop this campaign and related materials in partnership with organizations that have ties to underserved and hard-toreach communities. This includes the creation of modular content easily adapted for different languages, cultural contexts, and specific vulnerability profiles.

One-size-fits-all outreach campaigns often fail to resonate with different demographic groups or address specific consumer vulnerabilities. This leaves certain populations, especially those with language barriers, accessibility barriers, those in the senior community, disabled individuals, or different cultural contexts underserved and more vulnerable to scams and fraud. To maximize the reach and impact of awareness campaigns, the Commission could partner with a range of entities serving diverse communities to tailor messaging and outreach methods.

For example, the Commission can partner with organizations to:

- Conduct focus groups with various demographic segments, including but not limited to those outlined below, to ensure messaging resonates across different populations and is contextually and culturally competent.
- Utilize diverse representation in all campaign materials to increase relatability and engagement.
- Provide professionally translated²¹ materials in non-English languages, including but not limited to the following languages the Commission already provides translations for:
 - o <u>Arabic</u>,
 - <u>CHINESE-TRADITIONAL</u>,
 - <u>CHINESE-SIMPLIFIED</u>,
 - o <u>French</u>,
 - <u>HAITIAN-CREOLE</u>,
 - 0 <u>Korean</u>,
 - o <u>Portuguese</u>,
 - o <u>Russian</u>,
 - o <u>Spanish</u>,
 - o <u>TAGALOG</u>,

²¹ Materials should be translated using professional translation services that are linguistically and culturally competent. While AI tools are increasingly used for translation services, <u>research</u> has surfaced many key limitations in their deployment for this use case. *See* Nichols and Bhatia, <u>"Lost in Translation: Large Language Models in Non-English Content Analysis," *Center for Democracy and Technology*, May 23, 2023. <u>https://cdt.org/insights/lost-in-translation-large-language-models-in-non-english-content-analysis/</u></u>

- o <u>VIETNAMESE</u>, and
- American Sign Language.
- Develop audio descriptions of all visual materials alongside written materials to maximize accessibility for visually impaired individuals.
- Develop simplified versions of all materials for individuals with cognitive disabilities or limited literacy.
- Include content and formatting in campaign materials that follow best practices for older individuals, including larger font sizes, styles, and other recommended tools.

Additionally, consumer education and outreach campaigns should be consistent and reflect the lived realities of consumers. The key to durable and sustained campaigns is the creation of engaging, adaptive, and sustained materials and resources that empower consumers with knowledge and practical skills to protect themselves in an evolving threat landscape. Key factors to consider when developing materials and deployment strategies for large-scale education campaigns that meet consumers where they are could include:

- Prioritizing hands-on, interactive learning experiences tailored to the specific needs and pace of the target audience.
 - Many campaigns focus on distributing pamphlets or creating websites without ensuring active engagement. When designed this way, information often doesn't translate into behavior change or skill development. Instead, the Commission could co-develop handson workshops, simulations, and role-playing exercises with community anchor institutions that allow consumers to practice identifying and responding to AI-generated scams.
- Leveraging the reach and user engagement of popular platforms to deliver timely, relevant information.
 - Like any emerging technology, AI is rapidly evolving. Education campaigns must similarly be agile and follow trends in technology development to keep pace with the threats presented by potential misuse of these technologies, while also acknowledging the beneficial aspects and applications of technologies.
 - To keep pace with evolving trends, the Commission could establish a process for rapidly updating educational materials as new AI scam tools and techniques emerge, possibly leveraging AI itself to help identify and analyze new threats.
- Maintaining consistent messaging across multiple channels to reinforce key points through repetition and varied presentation.
 - AI-powered technologies, and the bad actors who use them, specifically exploit cognitive biases and vulnerabilities. Many campaigns focus on knowledge transfer without adequately addressing the psychological factors influencing risky online behaviors. Consumers may understand the risks but still engage in unsafe practices due to ingrained habits or cognitive biases.
- Fostering a sense of shared responsibility and leveraging existing community structures.
 - Some campaigns rely too heavily on scare tactics, which can lead to increased consumer fatigue or disengagement. Campaigns should balance preventative and proactive

messaging with community empowerment strategies that promote consumer and community-level resilience.

- While educating about risks, materials should emphasize the power of informed decisionmaking and provide clear, actionable steps for protection.
- Leaning into gamification techniques to make learning enjoyable and competitive while also encouraging repeated engagement with materials.

RECOMMENDATION #12: The CAC recommends that the Commission design a multichannel and multi-modal campaign dissemination plan to ensure broad reach and reinforcement of the education campaign. The Commission should develop a campaign dissemination plan in partnership with organizations that have ties to underserved and hard-toreach communities to maximize reach, accessibility, and impact.

A consumer education campaign is only as strong as the dissemination strategy that operationalizes it. Like the principles for creating inclusive and accessible campaign materials recommended above, it is critical that the Commission design a campaign implementation strategy using diverse communications mediums. Doing so builds campaign credibility and mainstreaming and lends itself to reinforcement learning for consumers once they see content and messaging across multiple channels. It also ensures that consumers with limited resources and media access can receive these campaign materials.

Dissemination tactics the Commission could consider to implement an education campaign include:

- > Print Newspaper, Magazines and Web-Only Publications
 - The Commission could include traditional print media outlets in its communications strategy, as well as web-only news outlets. Disseminating materials through these outlets ensures a broad audience. Since consumers tend to trust the outlets they read regularly, using these vehicles also enhances credibility of messaging. Tactics the Commission could leverage include:
- Publishing feature articles on AI-generated scams and protection strategies in national newspapers and web-only²² publications.
- Developing localized content for regional and local newspapers, highlighting regional scam trends and locally available community support resources.
- Placing informative posters and interactive kiosks in high-traffic areas like malls, airports, and public transportation hubs and with federal, state, and local agencies that provide direct services to consumers.
- Creating a regularly occurring column or newsletter dedicated to cybersecurity tips and recent scam alerts.
 - The Commission could collaborate with other federal agencies that produce materials or newsletters related to scams and fraud, such as the Federal Trade Commission.
- ➤ Mailers

A direct mailing program from the Commission will allow messaging to reach consumers who may not have access to national or local print news, or consumers with no or limited digital access, such as rural communities. A mailing program will ensure that remote communities' consumers who cannot access traditional media are reached.

²² Web-only publications include outlets like Axios news.

- A key target population for this program could include rural communities and landline-only or pay-as-you-go mobile users.
 - Ensuring that a dedicated phone number is available for these consumers to receive more information once they receive a mailer is critical.
- The Commission name, phone number, website, and email, should be clearly marked on the mailer and all materials to maintain credibility and legitimize the information delivered.
- Community-based organizations can also assist with distributing one-pagers, mailer copies, and related materials.
 - Partnering with community-based organizations in mailer distribution can further cement credibility of materials.

➤ Radio

Radio messaging is a traditional media channel that offers many benefits. Radio stations are often a reliable, trusted source with specific, loyal audiences for consumers that lack access to other forms of media. Many radio listeners also have long-standing relationships with radio hosts and personalities, enhancing the credibility of messaging. Radio messaging can also be especially impactful for consumers with limited literacy or internet access. Because radio stations are also regionally targeted and delivered, messaging can be tailored to fit certain demographics, like rural radio stations or non-English radio stations. Finally, radio messaging can be more cost-effective relative to other forms of dissemination like television or print news. Dissemination tactics the Commission could use over radio include:

- Producing regularly scheduled segments on AI scam prevention for syndication on national radio networks.
- Partnering with popular local radio personalities or hosts to share scam prevention tips during their shows, including non-English language and cultural radio programs, such as LGBTQ+ and faith-based programs.
- Hosting call-in shows with cybersecurity experts or trusted community leaders to answer listener questions.

> Podcasts

Podcasts offer similar benefits to radio programming, with some additional advantages. Since podcasts are on demand, messaging placed within podcasts can remain evergreen and received with more flexibility and accessibility for listeners. Podcasts are also generally serialized, tend to cover specialized topics, and have a longer format than radio programming, making them ideal for repeat engagement with listeners and building on listener loyalty. Podcasts are also easily shareable, through social media or messaging applications, increasing reach through word-of-mouth sharing. Finally, many platforms hosting podcasts offer transcripts or closed captioning, making content accessible to those with hearing impairments. Dissemination tactics the Commission can use through podcasts include:

- Launching a dedicated weekly podcast series on AI scams, digital literacy, and cybersecurity.
- Featuring interviews with victims, law enforcement, and cybersecurity and technology experts.
- Collaborating with existing popular technology, true crime, and consumer protection podcasts to reach diverse audiences.
- Collaborating with ethnic and non-English language podcasts, faith-based podcasts, and LGBTQ+ podcasts.

> Television

Television is another traditional communication medium that offers many benefits. Television news segments and public service announcements (PSA) can lend credibility and urgency to a campaign's messaging, reaching individuals who might not actively seek out this information through other channels. For older adults who may be less engaged with digital media but more vulnerable to certain scams, television remains a primary and trusted source of information. Television messaging also offers closed captioning for the deaf and hard of hearing and non-English speakers. By integrating television into the broader media mix, a campaign can ensure comprehensive coverage and reinforce its message across multiple touchpoints, maximizing overall effectiveness and public awareness. Dissemination tactics the Commission could use over television include:

- Producing primetime specials on national networks about the evolution of AI, scams, and their societal impact.
- Creating short, informative segments for morning shows and news broadcasts on local stations, including on non-English language channels.
- Developing PSAs for broadcast during high-viewership periods.
- Featuring local cybersecurity experts and victims in news segments on local stations.
- Placing PSAs on non-English language channels and dedicated cultural channels.

Social Media

Social platforms enable real-time and targeted dissemination of information about emerging AIgenerated scams, allowing for rapid response to new threats. The interactive nature of social media facilitates two-way communication, enabling the Commission to address public concerns directly and gather feedback. Moreover, social media's sharing capabilities can amplify the campaign's message through peer-to-peer networks, increasing trust and credibility. Social media dissemination tactics the Commission could use include:

- Leveraging platform-specific features like short-form videos, infographics, and live Q&A sessions to deliver content in diverse, engaging formats that resonate with different audience segments.
- Using appropriate and rights-respecting demographic targeting offered by social media platforms to reach individualized communities with culturally and contextually appropriate messaging.
- Partnering with creatives, cultural influencers and trusted community voices to promote consumer engagement and reach consumers in non-traditional cultural spaces.

> In-Person Events

An in-person engagement strategy remains crucial for education and awareness campaigns as it fosters direct, meaningful connections with consumers. Face-to-face interactions build trust and credibility and allow for nuanced discussions and immediate feedback that digital or broadcast media cannot replicate. These personal engagements provide opportunities to address local concerns, tailor messages to diverse community needs, and demonstrate the Commission's commitment to serving all consumers. Moreover, in-person events can reach populations with limited access to other media channels. By combining the authenticity of human interaction with the broad reach of other media strategies, an in-person approach strengthens the overall impact and effectiveness of the campaign. The Commission could:

- Co-host town hall meetings in various communities to discuss AI-generated scams and protection strategies throughout the life cycle of the education campaign.
- Conduct workshops at local libraries, community centers, faith-based institutions, schools, and senior and independent living centers, offering hands-on demonstrations of how to identify AI-generated calls and texts.
- Set up informational booths at community events, fairs, and farmers markets.
- Present at industry association events, including in collaboration with industry leaders.

RECOMMENDATION #13: The CAC recommends that the Commission should establish and maintain ongoing partnerships with community anchor institutions and organizations with strong community and grassroots ties in support of an education and awareness campaign.

Ongoing stakeholder engagement with community-based organizations can leverage existing trust networks and expertise to effectively reach diverse communities. These partnerships enable tailored messaging that resonates with specific groups, including those particularly vulnerable to AI-generated scams. This collaborative approach fosters the development of innovative educational resources and technological solutions, ensuring that the education campaign stays ahead of emerging threats. This strategy creates a sustainable, community-driven network of digital safety advocates, amplifying the campaign's impact and longevity. The Commission may also convene additional stakeholders, including educational institutions, other governmental agencies or bodies, and industry partners. The Commission could cultivate strong and diverse stakeholder partnerships by:

- Collaborating with libraries, community centers, community-based organizations, senior and independent living centers, faith-based institutions, and related community anchor institutions to host educational workshops.²³
- Partnering with organizations that work at the intersection of identity and technology, to raise awareness of particular concerns for communities that may be targeted.
- Partnering with local consumer protection agencies to tailor and amplify messaging and resources.
- Maximizing partnerships with groups structured to engage communities in the civic engagement space to elevate information about how AI robocalls and robotexts can be used to influence elections.^{24[4]}
- Developing curriculum modules for schools to teach students about AI-generated scams and digital literacy, including community colleges and adult education programs.
- Partnering with universities to research emerging AI scam techniques and effective prevention strategies.
- Offering training programs for educators to become "Digital Safety Ambassadors" in their communities.

²³ Including LGBTQ community centers via Centerlink and state organizations via the Equality Federation, and senior centers via SAGE.

²⁴ Such groups could include, for example, the LGBT Equality Caucus or Victory Fund Institute and similarly situated groups.

- Collaborating with workplaces and employers to implement AI scam awareness training for employees.
- Creating industry-specific guides on how AI-generated scams might target different professions.
- Working with smartphone manufacturers to develop best practices for integrating rightspreserving AI scam detection features into devices.
- Collaborating with AI companies to develop and implement ethical guidelines for voice cloning and other AI technologies.

RECOMMENDATION #14: The CAC recommends that the Commission develop a "train the trainers" model to grow community capacity and resilience to safely and appropriately respond to and report unwanted AI-generated robocalls and robotexts.

Once education and campaign materials are co-developed and disseminated with diverse stakeholder partners, the Commission could also consider growing community capacity by designing a "train the trainers" program that empowers consumers to train each other on the risks posed by AI-enabled robocalls and robotexts. Peer-driven learning offers many benefits and maximizes the reach and scale of a basic education campaign by adding new dimension and cultural and regional nuance to deployed education materials.

An established train-the-trainers model also provides a structured framework through which the Commission can add new or updated materials, including multidisciplinary topics like broadband literacy and other consumer priorities. These models can also serve as feedback loops to the Commission on emerging fraud trends or novel uses of AI-tools to exploit consumers. As part of a "train the trainer" program, the Commission could develop:

➤ A Comprehensive Training Curriculum

- The Commission could develop a modular curriculum covering AI technology, scam identification, and protection strategies mapped on to the general education materials developed in the above recommendation.
- The Commission could create slide decks, handouts, and interactive exercises for trainers. These materials can be used in the general education and awareness campaign, plus others developed specifically for this model.
- The Commission could work with community institutions to provide guidance on adapting materials for different audiences (e.g., seniors, youth, the disability community, and non-native English speakers).

➢ An Online Learning Platform

• The Commission could establish a centralized online resource hub where trainers can access and share training materials, best practices, case studies, and other relevant resources. This hub could be a continuous learning platform for trainers and their trainees, as well as a mechanism for the Commission to collect information on trends related to AI-generated robocalls and robotexts.

- This centralized hub can include a forum for trainers to share experiences and best practices. The Commission should periodically review these forums or meet with trainers to inform evolving best practices and identify new community or consumer needs.
- The Commission could offer webinars and virtual coaching modules for continuous trainer development.

> A Community-Based Organization Partnership Program

- The Commission could establish formal partnerships with diverse community-based organizations, including senior centers, independent living centers, libraries, community colleges, faith-based institutions, cultural organizations, and faith-based organizations to promote the train-the-trainers model and recruit trainers and trainees.
- The Commission could provide grants or stipends to community-based organizations for implementing AI scam education programs.
- The Commission could offer technical support and resources to community-based organizations for program implementation.

➤ A Feedback and Improvement Loop

- The Commission could implement regular surveys and focus groups with trainers and trainees for program feedback and to identify novel threats posed by the use of AI related to robocalls and robotexts.
- The Commission could analyze data on scam reports and prevention success rates to refine training materials.
- The Commission could host convenings for trainers and stakeholder partners to share insights, update strategies, and iterate on best practices.

RECOMMENDATION #15: The CAC recommends that the Commission integrate an AI robocall and robotext education campaign with broadband access and literacy initiatives.

Lack of exposure to and engagement with emerging technologies like AI is an extension of the digital divide. The Commission should leverage existing broadband access and literacy initiatives²⁵ and tools to reach consumers most vulnerable to AI-generated scams and fraud. Blending these topics can stretch the reach of these communications and leverage the existing credibility associated with these campaigns to further cement consumer engagement with materials. This strategy can be especially useful in reaching communities historically overrepresented in the digital divide, who may also be less well-versed in the risks associated with robocalls and robotexts.

²⁵ Initiatives to leverage can include the Homework Gap and Connectivity Divide initiative, the Rural Broadband Accountability Plan, or the Broadband Data Collection initiative, all conducted by the Commission.

RECOMMENDATION #16: The CAC recommends that the Commission expands and further promotes its Consumer Inquiries and Complaints Center.

Expanding and enhancing the FCC's Consumer Inquiries and Complaints Center is crucial for effectively combating AI-generated scams and protecting consumers. By improving visibility, streamlining processes, and leveraging technology, the Center can become a more accessible and responsive consumer resource. This approach empowers consumers to report issues quickly and enables the Commission to gather data on emerging threats to inform proactive measures and policy decisions. Moreover, the proposed improvements, including multilingual support and comprehensive demographic studies, ensure that the Center can serve diverse communities equitably, making it an indispensable tool in the fight against digital fraud. Some steps the Commission can take include:

- > Enhancing Visibility of The Commission's Consumer Inquiries and Complaints Center
- Integrate and link the Center within all education and messaging materials.
- Collaborate with telecommunications companies and industry associations to include information about the Center in customer and member communications.
- Develop a mobile application to easily access the Center's resources and complaint filing system.
- > Streamline the Commission's Complaint Process
- Simplify the online complaint form, making it more user-friendly and accessible for those with limited English language proficiency, and accessible on various devices and mediums.
- Implement AI-powered chatbots to guide users through the complaint process and provide instant responses to common inquiries. When AI-powered chatbots are used, consumers should be informed that they are communicating with a chatbot and given the option to "opt-out."
- Create a dedicated hotline for reporting AI-generated scam calls and texts.
- > Improve Response Times and Follow-Up Procedures at The Commission
- Increase staffing and resources to handle the growing volume of AI-related complaints.
- Implement an automated tracking system to keep consumers informed about the status of their complaints.
- Establish a rapid response team specifically for handling AI-generated scam reports.
- Regularly monitor complaints to timely identify topics for educational materials, outreach and education campaigns.

Comprehensive Demographic Study

- Conduct nationwide research to identify patterns in victimization across age, income, education, and geographic location.
- Analyze data from reported scams to identify common vulnerabilities or entry points used by scammers.
- •

APPENDIX 2024 FCC CAC Members

- Designated Federal Officer: Keyla Hernandez-Ulloa, Associate Chief, Consumer Affairs and Outreach Division, Consumer and Governmental Affairs Bureau (CGB), Federal Communications Commission
- Deputy Designated Federal Officer: **David M. Pérez**, National Community Impact Manager, Consumer Affairs and Outreach Division, CGB, Federal Communications Commission
- Former Designated Federal Officer: **Cara Grayer**, Attorney Advisor, Consumer Policy Division, CGB, Federal Communications Commission
- Former Deputy Designated Federal Officer, **Diana Coho**, Consumer Affairs and Outreach Specialist, Consumer Affairs and Outreach Division, CGB, Federal Communications Commission
- CAC Co-Chair: UnidosUS, Claudia Ruiz, Civil Rights Analyst
- CAC Co-Chair: National Consumers League, **John Breyault**, Vice President, Public Policy, Telecommunications and Fraud
 - o (Alternate) Eden Iscil, Public Policy Manager
- AARP, Dawit Kahsai, Government Affairs Director
 - o (Alternate) Coralette Hannon, Director, Livable Communities/Government Affairs
- American Cable Association (ACA Connects), Brian Hurley, Chief Regulatory Counsel

 (Alternate) Bill Tortoriello, Director of Regulatory Affairs
- Asian-Americans Advancing Justice AAJC, John Yang, President and Executive Director
 - (Alternate) Nicole Morgenstern, Telecommunications, Technology, and Media Policy Associate Manager
- AT&T, Linda Vandeloop, Assistant Vice President, External Affairs/Regulatory
 - o (Alternate) Angela DeMahy, Director, Federal Regulatory & External Legislative Affairs
- Individual, Cody Dorsey, Executive Director, Baltimore Digital Equity Coalition
- Common Sense, Amina Fazlullah, Senior Director of Equity Policy
- Consumer Technology Association, Rachel Sanford Nemeth, Senior Director Regulatory Affairs
 (Alternate) David Grossman, Vice President of Regulatory Affairs
- Deep East Texas Council of Governments, Mickey M. Slimp, Broadband Project Consultant
 - o (Alternate) Robert Bashaw, Public Information Officer, Regional Planner
- The Hispanic Federation, Brent Wilkes, Senior Vice President for Institutional Development
- INCOMPAS, Lindsay Stern, Attorney and Policy Advisor
 - (Alternate) Christopher Shipley, Executive Director of Public Policy
- Information Technology Industry Council (ITI), Katherine (Katie) McAuliffe, Senior Director, Policy Telecommunications
- The Kapor Center, Lili Gangas, Chief Technology Community Officer
 - LGBT Technology Institute, Kristen Kelley, Director of Programs
 - o (Alternate) Ellie Bessette, Director of Operations & Finance
- Massachusetts Department of Telecommunications & Cable, Joslyn Day, Director, Consumer Division

 (Alternate) William Bendetson, Presiding Officer, Legal Division
- Multicultural Media, Telecom, and Internet Council, Kenley Joseph, Tech and Telecom Policy Counsel

 (Alternate) Robert Branson, President and CEO
- National Association of Broadcasters (NAB), Liliana Rañón, Vice President External Affairs
 - o (Alternate) Larry Walke, Associate General Counsel
- National Association of Telecommunications Officers and Advisors (NATOA), **Mitsuko Herrera**, Planning, Policy and Special Projects at Montgomery County, Maryland
 - o (Alternate) Frederick Ellrod III, Director, Communications Policy and Regulation Division
- National Consumer Law Center (NCLC), Olivia Wein, Senior Attorney
 - (Alternate) Margot Saunders, Senior Attorney

- National Diversity Coalition, Faith Bautista, CEO and President
- Next Century Cities, Andrew Stutzman, Executive Director
 - o (Alternate) Ryan Johnston, Senior Policy Counsel
- Northern Virginia Urban League, Inc., Scott Alfred Price, Board Member
- Project GOAL, Debra Berlyn, Executive Director
- RuralRISE/National Center for Research Development (NCRD), **Tina Metzer**, Vice President and Co-Founder
 - o (Alternate) Joseph Kapp, President and Co-Founder
- TDIforAccess, AnnMarie Killian, Chief Executive Officer
- The Internet & Television Association (NCTA), Radhika Bhat, Vice President and Associate General Counsel
 - o (Alternate) Steven Morris, Vice President and Associate General Counsel
- The Trevor Project, Kasey Suffredini, Interim Senior Vice President of Prevention

 (Alternate) Casey Pick, Director of Law & Policy
- United States Telecom Association (USTelecom), Diana Eisner, Vice President, Policy and Advocacy
 - o (Alternate) Josh Bercu, Vice President, Policy & Advocacy