Federal Communications Commission

Intergovernmental Affairs Quarterly Webinar Briefing

Emmitt Carlton, Deputy Division Chief, Office of Intergovernmental Affairs

Consumer & Governmental Affairs Bureau

Federal Communications Commission

National Digital Connectivity & Lifeline Awareness Week

James Bradford Ramsay, General Counsel,
National Association of Regulatory Utility Commissioners (NARUC)

What is Digital Connectivity & Lifeline Awareness Week?

Digital Connectivity and Lifeline Awareness Week (formerly named Lifeline Awareness Week) is an annual outreach event that takes place the first full week after Labor Day in partnership with the National Association of Regulatory Utility Commissioners (NARUC) and National Association of State Utility Consumer Advocates (NASUCA). **This year DCLAW takes places September 8-14, 2024.**

The week is designed to both raise awareness of and increase participation in Lifeline. Promotion of this program is aimed at ensuring that no one is unable to connect to crucial services simply because they cannot afford it.

Resources to Support

- **NARUC's Toolkit:** https://www.naruc.org/about-naruc/our-programs/national-digital-connectivity-lifeline-awareness-week/
  - Governor Proclamation
  - Traditional Media Sample News Release, Public Service Announcement, & Letter to the Editor
  - Social Media Sample posts
  - Outreach Events and Promotional Materials
  - Sample Letter to Companies and Community Groups

- **FCC's Lifeline Program: https://www.fcc.gov/lifeline-consumers**
  - Consumer Guide
  - Social Media Graphics Coming Soon!

Ways You Can Engage:

1. **Email and/or text to your memberships**.
    - Share information about the Lifeline program.
    - Ask them to share their digital connectivity success stories and demonstrate the importance of closing the digital divide.
2. **Issue an official press release, proclamation, or video announcement** to show your organization's support.
    - Proclamations for Digital Connectivity and Lifeline Awareness Week (NARUC's toolkit offers a sample).
    - Lift the need for high-speed internet access and affordability for all families.
    - Highlight local success stories and impact of programs like Lifeline, and the need to continue to close the digital divide.
3. **Promote and share the Digital Connectivity & Lifeline Awareness Week content** on social media, blogposts, and websites.
    - Use sample posts in the NARUC toolkit or post your own content about how programs like Lifeline have helped millions of families across the country get connected.
    - Spread awareness about the Lifeline program's impact in their community.
    - Hashtags: #digitalconnectivity #lifelineawarenessweek
4. **Spread awareness about these programs through your existing programming.**
5. **Host a local or virtual awareness event** about the Lifeline program.

Federal Communications Commission

THANK YOU

James Bradford Ramsay, General Counsel
National Association of Regulatory Utility Commissioners (NARUC)
Wesley.Platt@fcc.gov

AI Generated Robocalls & Robotexts

CG Docket No: 23-239

Wes Platt, Chief, Consumer Policy Division, Information Access, & Privacy

Consumer & Governmental Affairs Bureau

AI NPRM & NOI

- **Adopted by the FCC on August 7, 2024.**
- **Comments and reply comments will be due 30 and 45 days, respectively, after publication in the Federal Register.**
- **The item represents the next step in the proceeding the FCC launched in November 2023 on the potential impacts of AI on its efforts to protect consumers from unwanted and illegal robocalls.**
- **As described in the following slides, the NPRM proposes measures to protect consumers from AI-generated robocalls, while the NOI seeks comment generally on certain types of AI technologies.**

AI NPRM & NOI

Federal Communications Commission

Proposes to define "AI-Generated Call" in the context of the TCPA

- For purposes of identifying the types of calls that would be subject to the new proposed rules, the NPRM proposes to define "AI generated call" as "a call that uses any technology or tool to generate an artificial or prerecorded 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."

Proposes to adopt new disclosure rules that would apply to AI-generated calls

- Callers making calls using AI-generated artificial or prerecorded voice messages would have to include clear and conspicuous disclosure that the consumer's consent to receive artificial and prerecorded calls may include consent to receive AI-generated calls;
- Callers making autodialed text messages that include AI-generated content would have to provide clear and conspicuous disclosure that the consumer's consent to receive such messages may include consent to receive AI-generated content; and
- Callers using AI-generated voice would have to, at the beginning of each call, clearly disclose to the called party that the call is using AI-generated technology.

AI NPRM & NOI

Proposes to remove impediments to beneficial uses of AI to promote access to telephone service by individuals with disabilities

- The NPRM proposes to exempt from the TCPA's requirements artificial or prerecorded voice calls made by an individual with a speech or hearing disability using any technology, including artificial intelligence technologies, designed to facilitate the ability of such individuals to communicate over the telephone.

Seeks comment on technologies that can assist consumers in avoiding illegal, unwanted, and AI-generated calls

- The NOI 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 use AI-generated voice based on real time analysis of call content; 2) alert consumers to the potential that such calls are fraudulent or AI-generated; and 3) potentially block future calls that can be identified as similar based on analytics.
- The draft NPRM also seeks comment on the privacy implications of real-time content-based call detection, alerting, and blocking technologies and whether the Commission should consider requirements to protect the privacy of called parties and callers, and, if so, what they should be.

Robocall Mitigation Database NPRM

- **Adopted by the FCC on August 7, 2024.**
- **Comments and reply comments will be due 30 and 60 days, respectively, after publication in the Federal Register.**
- **Launches a proceeding to examine ways to ensure and improve the overall quality of submissions into the Robocall Mitigation Database.**
  - Proposes and seeks comment on procedural measures that the FCC could adopt to promote the highest level of diligence when providers submit required information to the Robocall Mitigation Database, and technical solutions that the FCC could use to identify data discrepancies in filings—and require them to be corrected—before they are accepted by the system.
  - Proposes and seeks comment on measures to increase accountability for providers that submit inaccurate and false information to the Robocall Mitigation Database or fail to update their filings when the information they contain changes, as required by the FCC's rules.
  - Invites comment on any other procedural steps the FCC could require to increase the effectiveness of the Robocall Mitigation Database as a compliance and consumer protection tool.

Federal Communications Commission

THANK YOU

Wes Platt, Chief, Consumer Policy Division, Information Access, & Privacy
Consumer & Governmental Affairs Bureau
Wesley.Platt@fcc.gov

New Alert Code for Missing & Endangered Persons

Docket Nos: 15-91, 15-94

Theodore Marcus, Legal Advisor, Front Office
Consumer & Governmental Affairs Bureau

FCC's New "MEP" Event Code for Emergency Alerts (Docket Nos: 15-91, 15-94)

- **August 7, 2024 – Federal Communications Commission (FCC) - Report and Order**: The FCC Commissioners adopted a new event code for the Emergency Alert System (EAS) – the Missing and Endangered Persons ("MEP") event code.
  - While the FCC does not send the alerts, the FCC makes the operational rules for the communication providers who deliver the alerts to the public.

- **FCC's Decision**: (1) The MEP code will be an option in the EAS. (2) MEP alerts can also be sent to wireless phones, using existing methodologies in the Wireless Emergency Alert System or WEA.

- The MEP code will be available to help law enforcement agencies galvanize public attention to missing and endangered people of all ages who do not qualify for AMBER Alerts, including those who meet the criteria for Ashanti Alerts and Silver Alerts.

- This new code addresses a gap in nationwide emergency alerting regarding missing and endangered persons.
  - In 2023, the National Congress of American Indians passed a resolution asking the FCC to establish a code to enable a rapid and coordinated response to incidents involving missing indigenous persons.

How will this MEP Event Code work?

- Alert Originators (AOs), such as local public safety officials, first decide whether they will send an emergency alert. EAS alerts are used for events, such as hurricanes, tornados, earthquakes, and missing children.

- AOs use the Emergency Alert System by selecting an event code based on the nature of the situation. Just as they use "CAE" for "Child Abduction Emergencies" that warrant AMBER Alerts, they will be able to choose the "MEP" event code for "Missing and Endangered Persons."

- The MEP code will be used for persons who do not meet the criteria for an AMBER Alert (i.e., children 17 or younger and missing under circumstances that do not warrant an AMBER Alert or individuals over the age of 17 who are missing and endangered).

- Alert transmissions will also be able to map onto the existing Wireless Emergency Alert tools to send missing and endangered persons alerts to wireless phones.

- Tribes as well as state and local governments will be able to continue using their own alerts that have been adopted to help recover missing persons, including those adopted specifically for Missing & Murdered Indigenous Women & People (MMIWP).

MEP Alert Code – Timeline and Benefits

- **Rules to go into effect 12 months after publication** of the FCC's decision in the Federal Register (**imminent*).
  - EAS Participants (radio, cable TV, other broadcasters) and participating wireless carriers are required to implement the new code in their systems within this timeframe (e.g., via technology updates).
  - EAS Participants distribute emergency alerts on a voluntary basis (this will continue with MEP).

- **MEP Event Code Benefits**: Expected to create uniformity in the emergency alert process to locate missing, murdered, and endangered individuals and will facilitate the rapid dissemination of information about adults and children who have been reported missing to law enforcement agencies, media, and the public.

- **More information about this item can be found here:** https://www.fcc.gov/consumer-governmental-affairs/missing-and-endangered-persons-emergency-alert-system-code

- **If you have questions about this item please contact:** alerting@fcc.gov **or Native@fcc.gov**.

THANK YOU

Theodore Marcus, Legal Advisor, Front Office
Consumer & Governmental Affairs Bureau
Theodore.Marcus@fcc.gov

Incarcerated People's Communication Services (IPCS)

WC Docket Nos: 23-62, 12-375

Victoria Goldberg, Division Chief, Pricing Policy Division
Wireline Competition Bureau (WCB)

New Rate Caps for Audio and Video in the 2024 IPCS Order

Tier (ADP)	Audio (Permanent) (Per minute)		Video (Interim) (Per minute)	
	Current Caps	New Caps	Current Caps	New Caps
Prisons (any ADP)	$0.14	$0.06	N/A	$0.16
Large Jails (1,000+)	$0.16	$0.06	N/A	$0.11
Med. Jails (350-999)	$0.21	$0.07	N/A	$0.12
Small Jails (100-349)	$0.21	$0.09	N/A	$0.14
Very Small Jails (0-99)	$0.21	$0.12	N/A	$0.25

The Martha Wright-Reed Act called for the FCC to adopt just and reasonable IPCS rates and charges for all intrastate, interstate, and international audio and video IPCS, bringing rates and charges for intrastate communications and video communications within the FCC's jurisdiction for the first time.

- The Order lowers existing per-minute rate caps for audio IPCS and establishes initial interim per-minute rate caps for video IPCS, given the evolving nature of the video market.
- The Order sets separate rate caps for audio and video IPCS using five different tiers of facilities which account for differing cost characteristics of prisons and of different size jails.
- These rates were derived from industry-wide cost data submitted by IPCS providers collected in the Commission's 2023 Mandatory Data Collection.

For more information, see: https://www.fcc.gov/general/ics-data-collections

2024 IPCS Order - *Significant Reforms*

Site Commission Payments Prohibited

- The Order ends IPCS providers' practice of making site commission payments to carceral facilities that are passed through to consumers via higher rates, by prohibiting IPCS providers from paying any kind of site commissions in connection with IPCS and from entering into contracts for the same
- The Order also preempts all state and local laws and regulations requiring IPCS providers to pay site commissions associated with IPCS.

Safety and Security Costs Recovery

- When deciding the costs that can be recovered in the per minute rates, the Order limits the costs providers may recover related to safety and security measures to only those costs that the Commission finds are used and useful in the provision of IPCS.

Separate Ancillary Service Charges Prohibited

- The Order prohibits providers from imposing separate ancillary service charges on IPCS consumers.
- Previously the Commission allowed five types of ancillary service charges to be assessed, including charges to speak to a live customer service agent and charges to put money into an IPCS account.
- We now incorporate the costs of such ancillary services in the rate caps, and prohibit providers from imposing any separate ancillary service charges on IPCS consumers.

Incarcerated Calling Services, Going Forward

Federal Communications Commission

Additional Policy Achievements

- **Alternate Pricing Plans Allowed:** The Order permits providers to offer optional communications services pricing structures subject to conditions to protect and benefit IPCS consumers in addition to the required per minute pricing structure.
- **Accessibility Requirements:** The Order further strengthens the requirements for access to IPCS by incarcerated people with communication disabilities that the Commission adopted in 2022.
- **Consumer Disclosure and Inactive Accounts:** The Order strengthens existing consumer protections, including new requirements imposed on the providers to disclose rates and charges, make available consumers' statements of accounts on a monthly basis, and to provide timely refunds and notification requirements for accounts deemed inactive.

Compliance Dates Are Staggered:

- Generally, providers must comply with the new rate caps and site commission rules between Jan. 1, 2025 and Apr. 1, 2025, depending on the size of facility.
- These compliance dates are extended by an additional year (to 2026) for certain contracts that incorporate a legally-mandated site commission payment, and for contracts that may require a material renegotiation because of the new rules.

THANK YOU

Victoria Goldberg, Division Chief, Pricing Policy Division
Wireline Competition Bureau (WCB)
Victoria.Goldberg@FCC.gov

Cybersecurity Labeling Program

PS Docket No: 23-239

Zoe Li, Attorney Advisor, Cybersecurity and Communications Reliability Division
Public Safety and Homeland Security Bureau

Cybersecurity Labeling for IoT
PS Docket No. 23-239

- In March 15 the Commission adopted a framework for a voluntary cybersecurity labeling program for wireless consumer Internet of Things (IoT) products.
- The FCC is the program owner and will adopt standards and testing procedures for products to use the label based on NIST's Core Baseline 8425.
- FCC is supported by a Label Administrator, Cybersecurity Labeling Administrators, and CyberLABs.

Cybersecurity Labeling for IoT
Continued

Federal Communications Commission

Lead Administrator

Cybersecurity Label Administrators (CLAs)

CyberLABs

Must be accredited

The program is supported by a Lead Administrator, Cybersecurity Labeling Administrators (CLAs), and CyberLABs.

- Lead Administrator collaborates with stakeholders to make recommendations to the FCC on cybersecurity standards and testing procedures and label design etc.; and is responsible for developing a consumer education campaign.
- Cybersecurity Label Administrators (CLAs) are responsible for day-to-day management of the program (e.g., accepting and reviewing applications and test reports and approving/denying use of the FCC IoT Label).
- CyberLABs are responsible for testing products to demonstrate compliance to the IoT Cybersecurity Label requirements; may be a CLA-run testing lab, an independent testing lab, or a testing lab internal to the applicant, but it must be accredited to ISO/IEC 17025 and recognized by the Lead Administrator.

Label Overview

U.S. CYBER TRUST MARK

- The FCC IoT Label is **binary**: Products either qualify, or do not qualify, to bear the label.
- The IoT Label includes the **U.S. Cyber Trust Mark and a QR code**.
  - The QR code is linked to a decentralized, publicly available registry with consumer-friendly information about the security of the product.
  - Registry information is made available by manufacturers through a common Application Programming Interface (API).
- The location of the FCC IoT Label and specific label design (e.g., white spaces and size) will be part of multi-stakeholder process coordinated by Lead Administrator.

Process for FCC Label Approval

Federal Communications Commission

1

Applicant (e.g., manufacturer) has their eligible product tested by a CyberLAB.

2

Applicant submits an application with supporting documents (including CyberLAB test report) to a CLA requesting approval to use the FCC IoT Label.

3

CLA reviews the application, test report, and other supporting documentation and determines whether the IoT product meets the program requirements.

4

CLA approves or denies the application.

For more information please visit:

THANK YOU

Zoe Li, Attorney Advisor, Cybersecurity and Communications Reliability Division
Public Safety and Homeland Security Bureau (PSHSB)
Zoe.Li@fcc.gov

NPRM Open Comment Periods

Aliza Katz, Attorney Advisor, Front Office
Consumer & Governmental Affairs Bureau
Aliza.Katz@fcc.gov

Comments May Be Filed in the FCC's Electronic Comment Filing System

Quick Link to Submit Comments: https://www.fcc.gov/ecfs/filings/standard
Link to search comments: https://www.fcc.gov/edocs

When submitting comments to the FCC, be aware that:

- Comments should include your name.
- You must include the docket number or rulemaking number of the proceeding for the corresponding comment. The docket number or rulemaking number of the proceeding can be found on the first page of the FCC document or Public Notice opening the proceeding.
- You can file a comment both electronically and in paper format.
- Electronic comments must be filed by midnight Eastern Time on the date of the comment deadline.
- Written comments must be filed by 7p.m. ET on the date of the comment deadline.

SAVE THE DATES

Next IGA Quarterly Briefings:

- Thursday, October 31
- Thursday, January 30

If you would like to schedule a meeting with our subject matter experts or invite the FCC to attend an event or conference, please reach out to iga@fcc.gov.

FCC Participation at Upcoming Events & Conferences

- **Sept. 8-14:** National Digital Connectivity & Lifeline Awareness Week
- **Sept. 11-15:** Congressional Black Caucus Foundation's annual conference
- **Sept. 17-19:** Congressional Hispanic Caucus Institute's Leadership Conference
- **Sept. 25-26:** Asian Pacific American Institute for Congressional Studies' Tech Summit
- **Sept. 25-26:** National Governor's Association's Infrastructure Coordinator Quarterly Workshops
- **Sept. 30-Oct. 2:** National Association of Attorneys General's Fall Consumer Protection Conference

THANK YOU

Emmitt Carlton, Deputy Chief, Office of Intergovernmental Affairs
Consumer & Governmental Affairs Bureau
Emmitt.Carlton@fcc.gov

If you have any additional questions, please reach out to IGA@fcc.gov.