

Informe 2024 del Comité Asesor de Consumidores de la Comisión Federal de Comunicaciones

I. Resumen

El Comité Asesor de Consumidores (Consumer Advisory Committee, “CAC”) de la Comisión Federal de Comunicaciones (Federal Communications Commission, “FCC” o “la Comisión”) se complace en presentar el siguiente informe y recomendaciones a la FCC, en los que se examinan los usos de la inteligencia artificial (“IA”) para proteger a los consumidores de las llamadas automáticas no deseadas, los mensajes de texto automáticos y otros perjuicios, y para permitir que las personas con discapacidad puedan realizar llamadas. A lo largo de los últimos seis meses, el CAC se ha reunido tres veces en pleno y varias veces en grupos de trabajo para elaborar este informe. El CAC se basó en la experiencia de sus miembros, así como de expertos externos en inteligencia artificial, en la aplicación de la ley y en el acceso para personas con discapacidades a fin de elaborar las siguientes recomendaciones.

En su totalidad, este informe proporciona a la Comisión dieciséis recomendaciones individuales. Entre ellas, se incluyen recomendaciones para una mayor coordinación con otras agencias sobre soluciones integrales para proteger a los consumidores de la utilización de la IA en llamadas maliciosas; para la promoción de usos innovadores de la IA dirigidos a mejorar las tecnologías de bloqueo de llamadas; y la consideración de los riesgos para la privacidad, asociados al uso de herramientas de identificación y bloqueo de llamadas automáticas pregrabadas, en base al uso de la IA. En cuanto a la divulgación y a la educación, las recomendaciones del CAC incluyen una gestión, a nivel nacional, de información y educación pública, para capacitar a los consumidores de manera que puedan reconocer, reaccionar y efectuar denuncias de forma adecuada y segura cuando reciban llamadas o mensajes de texto automáticos no deseados o maliciosos. El informe también incluye una recomendación para que la Comisión integre una campaña de educación sobre llamadas o mensajes automáticos que utilizan la IA, junto con iniciativas que fomenten el acceso a la banda ancha y aporten conocimientos relacionados.

“La ansiedad que ocasionan estos avances tecnológicos es real, y con razón. Pero creo que cometemos un error si solo nos centramos en el potencial de daño. Tenemos que centrarnos igualmente en cómo la inteligencia artificial puede mejorar radicalmente las herramientas de que disponemos hoy para bloquear las llamadas y los mensajes de texto automáticos no deseados. Nos referimos a una tecnología que pueda ver patrones en el tráfico de nuestra red como nunca antes. Esto puede conducir al desarrollo de herramientas analíticas exponencialmente mejores para detectar el fraude antes de que llegue a nuestros hogares.

Si lo usamos a gran escala, no solo podremos detener estos elementos no deseados, sino que también podremos ayudar a restablecer la confianza en nuestras redes”.

- Jessica Rosenworcel, presidenta de la FCC (15 de noviembre de 2023)

II. Antecedentes

Como reconoció la presidenta de la FCC, Jessica Rosenworcel, la IA promete un gran potencial para los consumidores, incluso en la lucha contra las llamadas maliciosas¹. No obstante, en tiempos de aumento en las estafas², la IA también representa riesgos sustanciales para los consumidores, ya que los delincuentes la utilizan con malas intenciones.

El 28 de marzo de 2024, la presidenta de la FCC encargó al CAC de la FCC, ya en su duodécimo periodo, examinar los usos de la IA, cómo esta podría proteger a los consumidores de las llamadas y mensajes de texto automáticos no deseados y otros perjuicios, y cómo podría mejorar el acceso de las personas con discapacidad en la realización de llamadas. En concreto, la presidenta de la FCC encargó al Comité la elaboración de un informe que incluyera conclusiones sobre:

1. Cómo puede la Comisión ayudar a evitar que la IA se utilice con fines maliciosos.
2. Cómo se utiliza la IA para ayudar a los consumidores a evitar llamadas y mensajes de texto automáticos no deseados.
3. Cómo puede la Comisión promover esos usos.
4. Cómo se utiliza la IA para facilitar el acceso de las personas con discapacidad para hacer llamadas.
5. Cómo puede la Comisión fomentar los usos coherentes con las disposiciones de la ley de protección al consumidor de servicios telefónicos (Telephone Consumer Protection Act, TCPA) y garantizar que su futura labor contra las llamadas automáticas no sea un impedimento.
6. Qué actividades de divulgación o educación deberían llevarse a cabo para mantener a los consumidores informados sobre el desarrollo de estas tecnologías y aplicaciones.

III. Definiciones

La “inteligencia artificial” abarca una amplia gama de tecnologías y funciones y ha sido definida por diversas organizaciones de varias maneras.

¹ “Desde mi posición como jefa de la agencia experta en comunicaciones de nuestro país, no puedo evitar ser optimista sobre el futuro de la IA”. “Observaciones de la presidenta de la FCC, Jessica Rosenworcel, taller conjunto de la Comisión Federal de Comunicaciones y la Fundación Nacional de Ciencias”, Comisión Federal de Comunicaciones, 13 de julio de 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.”); <https://docs.fcc.gov/public/attachments/FCC-23-101A2.pdf> (“Tenemos que centrarnos igualmente en cómo la inteligencia artificial ;

“Tenemos que centrarnos igualmente en cómo la inteligencia artificial puede mejorar radicalmente las herramientas de que disponemos hoy para bloquear las llamadas y los mensajes de texto automáticos no deseados. Nos referimos a una tecnología que pueda ver patrones en el tráfico de nuestra red como nunca antes se ha hecho. Esto puede conducir al desarrollo de herramientas analíticas que sean exponencialmente mejores para detectar el fraude antes de que llegue a nuestros hogares. Si lo usamos a gran escala, no solo podemos detener estos elementos no deseados, sino que también podemos ayudar a restablecer la confianza en nuestras redes”. “Declaraciones de la presidenta de la FCC Jessica Rosenworcel sobre las implicaciones de las tecnologías de inteligencia artificial en la protección de los consumidores frente a llamadas y mensajes de texto automáticos no deseados”, Comisión Federal de Comunicaciones, 15 de noviembre de 2023.) <https://docs.fcc.gov/public/attachments/FCC-23-101A2.pdf>

² “As Nationwide Fraud Losses Top \$10 Billion in 2023, FTC Steps Up Efforts to Protect the Public” (Las pérdidas por fraude a nivel nacional superan los 10 mil millones de dólares en 2023, y la Comisión Federal de Comercio [Federal Trade Commission, FTC] intensifica sus esfuerzos para proteger al público), Comisión Federal de Comercio, 9 de febrero de 2023. <https://www.ftc.gov/news-events/news/press-releases/2024/02/nationwide-fraud-losses-top-10-billion-2023-ftc-steps-efforts-protect-public>

En el Código de Estados Unidos se define la inteligencia artificial (15 U.S. Code § 9401) como un “sistema basado en una máquina que puede, para un conjunto dado de objetivos definidos por el ser humano, hacer predicciones, recomendaciones o tomar decisiones que influyen en entornos reales o virtuales. Los sistemas de inteligencia artificial utilizan entradas basadas en máquinas y seres humanos para: A) percibir entornos reales y virtuales; B) abstraer esas percepciones en modelos mediante análisis de forma automatizada; y C) utilizar la inferencia de modelos para formular opciones de información o acción”.

La Comisión ha propuesto definir una llamada o texto generado por IA como “una llamada que utiliza cualquier tecnología o herramienta para generar artificialmente una voz o un texto utilizando tecnología computacional u otro aprendizaje automático, lo que incluye algoritmos predictivos y extensos modelos de lenguaje, para procesar el lenguaje natural y producir contenido de voz o texto para comunicarse con un receptor a través de una llamada telefónica saliente”³.

Este informe utilizará las definiciones anteriores. El CAC no asume ninguna posición sobre el mérito de estas definiciones.

IV. Hallazgos

1. ¿Cómo puede la Comisión ayudar a evitar que la IA se utilice para realizar llamadas maliciosas?

En consonancia con la acusación del CAC, este informe se centra en el uso de la IA para “fines de llamadas maliciosas”. A los efectos de este informe, la interpretación del CAC de “fines de llamadas maliciosas” se basa en la ley de protección al consumidor de servicios telefónicos (Telephone Consumer Protection Act, TCPA) y la ley para la veracidad en la identificación de llamadas (Truth in Caller ID Act). Entre otras cosas, la TCPA exige el consentimiento expreso previo para que una persona que llama pueda realizar una llamada utilizando un sistema de marcación telefónica automática o una voz pregrabada o artificial a un consumidor⁴. La FCC aclaró recientemente que una llamada realizada con una voz generada por IA es una “voz artificial” a efectos de la TCPA⁵, y más recientemente ha solicitado comentarios sobre la definición de “voz generada por IA”⁶. La ley para la veracidad en la identificación de llamadas considera ilegal transmitir información engañosa o inexacta sobre la identificación de

³ “Implications of Artificial Intelligence Technologies on Protecting Consumers from unwanted Robocalls and Robotexts” (Implicancias de las tecnologías de inteligencia artificial en la protección de los consumidores frente a llamadas y mensajes de texto automáticos no deseados), Comisión Federal de Comunicaciones, 17 de julio de 2024. <https://docs.fcc.gov/public/attachments/DOC-404036A1.pdf>

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

⁵ “In the Matter of Implications of Artificial Intelligence Technologies on Protecting Consumers from Unwanted obocalls and Robotexts” (Sobre las implicancias de las tecnologías de inteligencia artificial en la protección de los consumidores frente a llamadas y mensajes de texto automáticos no deseados), Comisión Federal de Comunicaciones, 8 de febrero de 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” (Implicancias de las tecnologías de inteligencia artificial en la protección de los consumidores frente a llamadas y mensajes de texto automáticos no deseados), Comisión Federal de Comunicaciones, 17 de julio de 2024. <https://docs.fcc.gov/public/attachments/DOC-404036A1.pdf>;

“FCC Launches Inquiry into AI’s Impact on Robocalls and Robotexts,” (La FCC inicia una investigación sobre el impacto de la IA en las llamadas automáticas y los mensajes de texto automáticos), Comisión Federal de Comunicaciones, 28 de agosto de 2024. <https://www.fcc.gov/consumer-governmental-affairs/fcc-launches-inquiry-ais-impact-robocalls-and-robotexts>

llamadas (es decir, una “suplantación de identidad”) con la intención de defraudar, causar daño u obtener ilícitamente algo de valor”⁷. Las recomendaciones del CAC pueden aplicarse a las llamadas generadas por IA que infrinjan alguno de estos estatutos o ambos.

RECOMENDACIÓN N.º 1: La FCC debería asociarse con otras agencias federales y con la Casa Blanca para garantizar la existencia de una solución global en todas las agencias que ayude a impedir que la IA se utilice con fines de llamadas maliciosas.

Utilizando las leyes mencionadas como guía, este informe considera “actividades de llamadas maliciosas” a las actividades de llamadas que transgredan la TCPA (p. ej., llamadas o mensajes de texto automáticos no solicitados), así como llamadas que suplantán la identidad con la intención de defraudar, causar daño u obtener ilícitamente algo de valor del consumidor. Las llamadas fraudulentas realizadas mediante IA pueden, por ejemplo, constituir una transgresión tanto de la TCPA como de la ley para la veracidad en la identificación de llamadas (Truth in Caller ID Act), así como de otras leyes (p. ej., leyes penales de fraude).

Nota: A fines de brevedad, cuando este informe se refiere a “llamadas automáticas”, se refiere tanto a llamadas automáticas como a mensajes de texto automáticos, a menos que se indique lo contrario. Esto es coherente con la Resolución y Orden Declaratoria Omnibus de la TCPA de 2015 de la Comisión (“En esta resolución y orden declarativa, nos referimos a las llamadas que requieren el consentimiento del consumidor de conformidad con la TCPA como “llamadas automáticas”, “llamadas y textos cubiertos” o “llamadas y textos de voz”).⁸

Históricamente, los ejemplos de llamadas maliciosas pueden dividirse en al menos dos tipos principales. En primer lugar, las llamadas maliciosas pueden ser (i) de gran volumen, en las que el delincuente llama aleatoriamente al mayor número posible de personas, o (ii) selectivas, en las que el delincuente llama a personas concretas conocidas.⁹ En segundo lugar, las llamadas maliciosas pueden ser (i) telemarketing ilegal que transgrede la TCPA y otras leyes de telemarketing y en las que se vende algún producto o servicio real¹⁰, (ii) fraude criminal manifiesto en el que el delincuente intenta utilizar un pretexto para

⁷ “Truth in Caller ID Act of 2009,” *Library of Congress*, December 22, 2010. (Ley de 2009 para la veracidad en la identificación de llamadas, Biblioteca del Congreso, 22 de diciembre de 2010). <https://www.congress.gov/111/plaws/publ331/PLAW-111publ331.pdf>

⁸ “In the Matter of Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991” (Sobre las normas y reglamentos que implementan la ley de 1991 para la protección del consumidor de servicios telefónicos), Comisión Federal de Comunicaciones, 10 de julio de 2015). <https://docs.fcc.gov/public/attachments/FCC-15-72A1.pdf>

⁹ “Prepared Testimony of Joshua M. Bercu...Hearing on Protecting Americans from Robocalls,” (Testimonio preparado de Joshua M. Bercu... Audiencia sobre cómo proteger a los estadounidenses de las llamadas automáticas), Subcomité de comunicaciones, medios y banda ancha, del Comité de comercio, ciencia y transporte del Senado de los EE. UU., 24 de octubre de 2023. <https://www.commerce.senate.gov/services/files/9E0BFE0C-E920-4C89-BE35-B2A4A8396181>, “Re: Enforcement Bureau Requests Information on the Status of Private-Led Traceback Efforts of Suspected Unlawful Robocalls” (Asunto: la oficina de aplicación de normas solicita información sobre el estado de los esfuerzos privados de rastreo de presuntas llamadas automáticas ilegales), Comisión Federal de Comunicaciones, 13 de noviembre de 2023. <https://www.fcc.gov/ecfs/document/11130588416636/1>

¹⁰ “FCC Closes TCPA Lead Generator Loophole; Requires One-to-One Consent” (La FCC cierra la laguna jurídica de la TCPA sobre los generadores de clientes potenciales; exige el consentimiento individual), Orrick, 20 de diciembre de 2023. <https://www.orrick.com/en/Insights/2023/12/FCC-Closes-TCPA-Lead-Generator-Loophole-Requires-One-to-One-Consent>

acceder directamente a las cuentas financieras de una persona o hacer que esta le envíe fondos¹¹.

Aunque el uso de la IA por parte de los delincuentes, para realizar llamadas maliciosas es todavía incipiente, hay muchas razones para creer que estos utilizarán la IA para todas las actividades de llamadas maliciosas descritas anteriormente. Y aunque hay pocas pruebas y datos públicos concretos disponibles sobre cómo los delincuentes utilizan la IA y a qué escala, las tecnologías de IA pueden ofrecer a los estafadores las siguientes posibilidades como parte de sus esfuerzos para realizar llamadas maliciosas:

Clonación de voz, mediante inteligencia artificial, para cometer fraudes. La clonación de voz -la capacidad de generar un clon de voz casi perfecto a partir de un breve clip de audio o fragmento de la voz de alguien- ofrece un enorme potencial para ayudar a las personas, entre ellas las que tienen alguna discapacidad, como se describe más adelante. Sin embargo, como ha señalado la FTC, “en las manos equivocadas, las tecnologías de clonación de voz pueden hacer daño”. Por ejemplo, la estafa de la emergencia familiar, en la que un impostor se hace pasar por un pariente en apuros. Un estafador podría clonar una voz que suene igual que la de su ser querido. Los estafadores también podrían clonar la voz de un director general u otro ejecutivo de la empresa a fin de engañar a los empleados para que transfieran grandes sumas de dinero o paguen una factura falsa¹².

- ***Clonación de voz a gran escala con fines fraudulentos o maliciosos.*** La Comisión abordó recientemente las denuncias de llamadas automáticas que supuestamente contenían una grabación de audio falsificada, generada por IA (*deepfake*, en inglés) de la voz del presidente Biden, en la que decía a los posibles votantes que no votaran antes de las elecciones primarias presidenciales de New Hampshire de 2024¹³.
- ***Aumento histórico en el volumen de llamadas maliciosas dirigidas.*** A efectos de fraude selectivo o telemarketing ilegal selectivo, la IA puede permitir a los delincuentes ampliar lo que de otro modo serían actividades de llamadas más limitadas. Históricamente, este tipo de llamadas y mensajes de texto dirigidos han implicado a una persona, la que llama o envía un mensaje en vivo (o un operador en vivo que utiliza un sistema de sonido) para reaccionar de la forma más natural posible ante la persona que recibe la llamada. Las llamadas y los mensajes de texto con IA permitirían a los delincuentes aumentar el número de conversaciones de este tipo,

¹¹ “Prepared Testimony of Joshua M. Bercu...Hearing on Protecting Americans from Robocalls” (Testimonio preparado de Joshua M. Bercu... Audiencia sobre cómo proteger a los estadounidenses contra las llamadas automáticas), Subcomité de comunicaciones, medios y banda ancha del Comité de comercio, ciencia y transporte del Senado de los EE. UU., 24 de octubre de 2023. <https://www.commerce.senate.gov/services/files/9E0BFE0C-E920-4C89-BE35-B2A4A8396181>, “Re: Enforcement Bureau Requests Information on the Status of Private-Led Traceback Efforts of Suspected Unlawful Robocalls,” (Asunto: la oficina de aplicación de normas solicita información sobre el estado de los esfuerzos privados de rastreo de presuntas llamadas automáticas ilegales); Comisión Federal de Comunicaciones, 13 de noviembre de 2023. <https://www.fcc.gov/ecfs/document/11130588416636/1>

¹² “Announcing the FTC’s Voice Cloning Challenge” (Anuncio del desafío de la FTC sobre la clonación de voz), Comisión Federal de Comunicaciones, 16 de noviembre de 2023. <https://consumer.ftc.gov/consumer-alerts/2023/11/announcing-ftcs-voice-cloning-challenge>

¹³ “FCC Proposes \$6 Million Fine for Illegal Robocalls That Used Biden Deepfake Generative AI Voice Message” (La FCC propone una multa de \$6 millones por las llamadas ilegales que utilizan mensajes falsificando la voz de Biden con el uso de IA), Comisión Federal de Comunicaciones, 23 de mayo de 2024. <https://docs.fcc.gov/public/attachments/DOC-402762A1.pdf>

aparentemente naturales, pero totalmente dirigidas.

- **Mejora en la calidad de las estafas.** La IA puede ayudar a los delincuentes a mejorar la calidad de sus estafas, ya sea mediante la clonación de voz con IA o, más sencillamente, mejorando los guiones de llamadas o mensajes de texto. Por ejemplo, la IA permitiría a los delincuentes cuyo idioma materno no es el inglés mejorar sus maniobras para estafar, al eliminar errores gramaticales comunes que son una señal de aviso a los angloparlantes de que el remitente de un mensaje puede no ser estadounidense.

RECOMENDACIÓN N.º 2: El CAC recomienda que la FCC declare explícitamente que una llamada realizada con una voz generada por IA con la intención de defraudar, perjudicar o engañar al destinatario infringe siempre la TCPA, ya que ningún consumidor razonable consentiría deliberadamente una llamada de este tipo realizada con una voz artificial.

En cuanto a la clonación de voz, la FCC ya ha dado un paso importante para hacer frente a esta amenaza: a saber, la resolución declaratoria del 8 de febrero de 2024 (February 8, 2024 Declaratory Ruling), confirmando que las restricciones de la TCPA sobre el uso de “voz artificial o pregrabada” abarcan las actuales tecnologías de IA que generan voces humanas, como las tecnologías de clonación de voz, y por lo tanto requieren el consentimiento expreso previo de la parte a la que se hace la llamada, para iniciar esas llamadas en ausencia de un propósito de emergencia o una exención¹⁴. La aplicación estricta de las normas de la Comisión sobre llamadas automáticas ilegales, lo que incluye la TCPA, los mecanismos adicionales de bloqueo y confiscación que la Comisión tiene la intención de adoptar en septiembre de 2024, la colaboración con los fiscales generales estatales para aumentar los recursos y la capacidad de aplicación, y la utilización de los datos de las quejas de los consumidores compartidos por la Comisión Federal de Comercio (“FTC”) contribuirían a este esfuerzo. Además, aumentar las multas por fraude también podría tener un efecto disuasorio. Recomendamos que la FCC estudie formas adicionales de apoyar la labor de los proveedores de servicios de voz para identificar y bloquear estas llamadas ilegales.

Además, la FCC ha iniciado una propuesta de normativa para aplicar las restricciones de la TCPA a las llamadas y a los mensajes de texto automáticos generados por IA¹⁵ así como un aviso de investigación para recopilar información adicional sobre las herramientas que se están desarrollando y cómo estas pueden introducirse en el ecosistema¹⁶.

El CAC espera con interés ver la evolución del expediente a medida que la Comisión estudia si debe

¹⁴ “In the Matter of Implications of Artificial Intelligence Technologies on Protecting Consumers from Unwanted Robocalls and Robotexts” (Sobre las implicancias de las tecnologías de inteligencia artificial en la protección de los consumidores frente a llamadas y mensajes de texto automáticos no deseados), Comisión Federal de Comunicaciones, 8 de febrero de 2024. <https://docs.fcc.gov/public/attachments/FCC-24-17A1.pdf>

¹⁵ “Implications of Artificial Intelligence Technologies on Protecting Consumers from Unwanted Robocalls and Robotexts,” (Implicancia de las tecnologías de inteligencia artificial en la protección de los consumidores frente a llamadas y mensajes de texto automáticos no deseados), Comisión Federal de Comunicaciones, 17 de julio de 2024. <https://docs.fcc.gov/public/attachments/DOC-404036A1.pdf>

¹⁶ “FCC Launches Inquiry into AI’s Impact on Robocalls and Robotexts,” (La FCC inicia una investigación sobre el impacto de la IA en las llamadas automáticas y los mensajes de texto automáticos), Comisión Federal de Comunicaciones, 28 de agosto de 2024. <https://www.fcc.gov/consumer-governmental-affairs/fcc-launches-inquiry-ais-impact-robocalls-and-robotexts>

exigir a las personas que llaman, al obtener el consentimiento expreso previo, que revelen al destinatario que tienen la intención de utilizar llamadas y mensajes de texto generados por IA, y si debe exigir que algunas llamadas generadas por IA deban incluir dicha revelación durante la llamada. Además, el CAC recibe con satisfacción la consideración de la Comisión sobre cómo se aplican la TCPA y otras restricciones a estas tecnologías y qué usos deberían quedar exentos. El CAC también aplaude el esfuerzo de la Comisión por garantizar que las personas con discapacidad puedan utilizar las tecnologías de IA sin necesidad de obtener previamente el consentimiento expreso del destinatario de sus llamadas.

Los esfuerzos de las agencias para promover el desarrollo de esas herramientas han logrado resultados notables. Por ejemplo, el Federal Trade Commission's Voice Cloning Challenge (“Desafío de la Comisión Federal de Comercio, sobre la clonación de voz”) otorgó premios en dinero a entidades que desarrollaron productos, políticas y procedimientos destinados a proteger a los consumidores de los daños causados por la clonación de voz mediante IA. El desafío de la FTC estaba dirigido a fomentar ideas innovadoras sobre prevención, control y evaluación de la clonación maliciosa de voces¹⁷.

RECOMENDACIÓN N.º 3: El CAC recomienda que la Comisión considere impulsar, posiblemente de manera acelerada, un taller, exhibición u otra iniciativa para alentar a los proveedores de servicios de voz, proveedores de análisis y otras partes interesadas, a desarrollar, demostrar e implementar tecnologías de detección y mitigación de IA, para bloquear llamadas identificadas como susceptibles de contener clonación de voz con IA.

2. ¿Cómo se utiliza la IA para ayudar a los consumidores a evitar las llamadas y los mensajes de texto automáticos no deseados?

A lo largo de la última década, además de otras medidas gubernamentales, la FCC ha trabajado con los proveedores de comunicaciones en el despliegue de numerosas herramientas para proteger a los consumidores, de las llamadas y los mensajes de texto automáticos no deseados. Entre estas se incluye:

- Análisis de bloqueo y etiquetado, disponible gratuitamente para bloquear llamadas directamente o dar a los consumidores información que les ayude a tomar la decisión de contestar o no una llamada.
- Bloqueo a nivel de la red.
- El marco de autenticación del identificador de llamadas de la identidad telefónica segura revisada (Secure Telephone Identity Revisited, STIR) / del manejo basado en firmas de información afirmada usando identificadores (Signature-based Handling of Asserted Information Using toKENS, SHAKEN; “The STIR/SHAKEN caller ID authentication framework”, en inglés).
- Conozca a su cliente (Know your Customer, “KYC”) y conozca a su proveedor de servicios (Know-Your-Upstream-Provider, “KYP”).
- Rastreo de la industria.

Además de las que ofrecen los proveedores de comunicaciones, las aplicaciones de alto nivel ofrecen opciones adicionales para los clientes. Por ejemplo, el servicio de bloqueo de llamadas automáticas YouMail utiliza IA para identificar llamadas y mensajes de texto no deseados de estafas y telemarketing. Luego puede bloquear estos mensajes para sus propios clientes minoristas. Sin embargo, lo que es aún más importante es que YouMail trabaja con diferentes actores a lo largo de las vías de llamadas y

¹⁷ “The FTC Voice Cloning Challenge” (Desafío de la FTC sobre la clonación de voz), Comisión Federal de Comunicaciones (FTC), <https://www.ftc.gov/news-events/contests/ftc-voice-cloning-challenge>

mensajes de texto para notificarles estas llamadas y mensajes no deseados, de modo que puedan bloquearse para todos los destinatarios. El sistema de YouMail impulsado por inteligencia artificial analiza patrones y comportamientos asociados con el mercadeo no deseado y las llamadas fraudulentas, mediante el empleo de algoritmos de aprendizaje automático para identificar y filtrar estas comunicaciones no deseadas, de manera más efectiva.

En muchos casos, las analíticas de bloqueo y etiquetado se basan en el aprendizaje automático, una forma de automatización que no es IA generativa. Si bien la IA generativa es una herramienta poderosa, no es necesariamente la mejor solución para todos los problemas. Por ejemplo, el CAC recibió comentarios de un experto en el uso de la IA por parte de los proveedores de servicios de voz en el sentido de que los proveedores también pueden utilizar el aprendizaje automático y otro tipo de automatización, como la IA discriminativa, como parte de sus procesos de bloqueo de red y de KYC y KYP¹⁸.

La mayoría de las herramientas de mitigación de llamadas automáticas y mensajes de texto automáticos implementadas actualmente en la industria son independientes de la tecnología y están destinadas a identificar y detener llamadas y mensajes de texto maliciosos, sin importar si los creadores de esas llamadas o mensajes de texto utilizaron IA para producirlas. Las analíticas de bloqueo y etiquetado implementadas por el proveedor, por ejemplo, detectan patrones de llamadas sospechosos y toman medidas cuando se identifican dichos patrones, sin depender del contenido de la llamada, ya que los proveedores no pueden escuchar el contenido de todas las llamadas ni legal ni técnicamente. Estas herramientas pueden proteger eficazmente a los consumidores contra las actividades de llamadas maliciosas generadas por la IA, ya que pueden identificar patrones sospechosos, como un gran volumen de llamadas y mensajes de texto de la IA, y su uso debería promoverse.

Del mismo modo, los proveedores de servicios toman medidas para investigar a sus clientes y proveedores de servicios de voz inmediatos, lo que ayuda a reducir el tráfico malicioso en sus redes, independientemente de si dicho tráfico está generado por IA o no. Por último, los proveedores de servicios están obligados a cooperar con el Industry Traceback Group (“ITG”), que identifica a las entidades responsables de llamadas ilegales, sin importar que dichas llamadas sean suplantadas. En 2024, el ITG rastreó una campaña ilegal de llamadas automáticas que clonó la voz del presidente Joe Biden, lo que ayudó a que la FCC aplicara medidas contra la parte que llamaba y el proveedor responsable de originar las llamadas¹⁹.

Las tecnologías nuevas y emergentes se centran en identificar voces sintéticas o identificar con marcas de agua voces clonadas legalmente. El año pasado, la FTC lanzó un desafío sobre clonación de voces para identificar herramientas que puedan ayudar a detectar voces clonadas maliciosamente. Las candidaturas ganadoras propusieron herramientas útiles para detectar voces sintéticas que utilizan algoritmos de IA para detectar las diferencias sutiles entre patrones de voz auténticos y sintéticos, formas de marca de agua para dificultar la clonación con precisión y una técnica que autentifica el origen humano de las grabaciones de voz cuando se crean y luego incrusta esta autenticación como marca de agua o firma en la transmisión. El participante que obtuvo el segundo lugar desarrolló una tecnología que detecta en tiempo real los clones de voz y los audios falsificados, generados por IA (*deepfakes*, en inglés)²⁰.

¹⁸ Presentación de Greg Bohl, director de datos de Transaction Network Services, ante el Comité Asesor de Consumidores de la Comisión Federal de Comunicaciones, 7 de junio de 2024.

¹⁹ “FCC Proposes \$6 Million Fine for Illegal Robocalls That Used Biden Deepfake Generative AI Voice Message,” (La FCC propone una multa de \$6 millones por las llamadas ilegales que utilizan mensajes falsificando la voz de Biden con el uso de IA), Comisión Federal de Comunicaciones, 23 de mayo de 2024. <https://docs.fcc.gov/public/attachments/DOC-402762A1.pdf>

²⁰ “The FTC Voice Cloning Challenge” (Desafío de la FTC sobre la clonación de voz), Comisión Federal de Comercio (FTC). <https://www.ftc.gov/news-events/news/press-releases/2024/04/ftc-announces-winners-voice-cloning-challenge>

A medida que el Gobierno sigue fomentando el desarrollo y el uso de herramientas de IA para mitigar las comunicaciones fraudulentas, el CAC también insta a la Comisión a considerar cómo pueden utilizarse las herramientas de IA para servir al doble propósito de reducir los incidentes de falsos positivos y el bloqueo o etiquetado erróneo del tráfico legítimo.

RECOMENDACIÓN N.º 4: El CAC recomienda que la Comisión siga apoyando el despliegue, por parte de los proveedores de servicios de voz, de herramientas y procesos actuales y adicionales para identificar, bloquear, etiquetar (según corresponda) y mitigar de otro modo las llamadas y los mensajes de texto ilegales y no deseados, lo que incluye los generados por IA, garantizando al mismo tiempo mecanismos de reparación adecuados para las personas que realizan llamadas.

Además, en su notificación de propuesta normativa (Notice of Proposed Rulemaking, NPRM) publicada el 8 de agosto de 2024, la FCC señala nuevas herramientas en desarrollo:

El expediente destaca varios ejemplos de tecnologías de detección de llamadas y alerta que pueden ayudar a detectar llamadas fraudulentas o que utilicen voz generada por IA en base al análisis en tiempo real del contenido de la llamada entrante. Por ejemplo, Google ha anunciado que está “probando una nueva función de control de llamadas que avisará a los usuarios si es probable que la persona con la que están hablando esté intentando estafarlos, y los animará a poner fin a tales llamadas”. Esta tecnología “utilizará Gemini Nano -una versión reducida del gran modelo lingüístico Gemini de la empresa para dispositivos Android que puede ejecutarse localmente y sin conexión- para buscar lenguaje fraudulento y otros patrones de conversación típicamente asociados a las estafas. Los usuarios recibirán alertas en tiempo real durante las llamadas en las que estén presentes estas señales de alarma”. Otras tecnologías en desarrollo tratan de autenticar la voz humana como método para frustrar las llamadas con voces generadas por IA, como las llamadas con fines fraudulentos que no revelan el uso de IA”.

Entre otras herramientas citadas por la Comisión se encuentran:

“Azure Operator Call Protection” (protección de llamadas de operadora Azure) de Microsoft. Es un servicio basado en datos que se ofrece a los proveedores de servicios telefónicos a nivel de red y que “detecta posibles estafas telefónicas, realiza análisis en tiempo real, en base a IA, de las llamadas telefónicas dirigidas a los consumidores, y alerta a los suscriptores cuando corren riesgo de ser estafados”.

RECOMENDACIÓN N.º 5: El CAC recomienda que la Comisión considere cómo los riesgos para la privacidad y el cumplimiento de las leyes de privacidad pueden verse afectados por el uso de tecnologías de detección de llamadas y alertas que supervisan el contenido de las llamadas realizadas a los consumidores mientras la Comisión evalúa los beneficios potenciales de estas.

3. ¿Cómo puede la Comisión promover esos usos?

Como ya se dijo, las tecnologías de IA todavía son emergentes y el uso de la IA por parte de los delincuentes está evolucionando rápidamente. La Comisión debe mantenerse al día con estos cambios para proteger más adecuadamente a los consumidores.

RECOMENDACIÓN N.º 6: El CAC recomienda que la Comisión considere la posibilidad de solicitar de manera periódica comentarios sobre el estado del entorno de las amenazas de llamadas y mensajes de texto generados por IA y las tecnologías que se están utilizando o desarrollando para enfrentar estas amenazas.

RECOMENDACIÓN N.º 7: El CAC recomienda que la Comisión promueva la colaboración entre los proveedores de servicios de voz, los desarrolladores de aplicaciones, los fabricantes de teléfonos y pertinentes, a fin de desarrollar herramientas que puedan ayudar a identificar y combatir la IA utilizada para realizar llamadas maliciosas.

En la medida que las entidades desarrollen herramientas que permitan supervisar y analizar el contenido de las llamadas para detectar estafas o las prácticas de llamadas maliciosas, la Comisión debería animar a estas entidades a estudiar la mejor manera de ofrecer transparencia y control a los consumidores, mitigando al mismo tiempo los riesgos para la privacidad.

RECOMENDACIÓN N.º 8: El CAC recomienda que la Comisión encargue a un futuro comité consultivo (que incluya a representantes de los consumidores) la elaboración de un informe en el que se examinen temas específicos relacionados con la aplicación de la IA por parte de las partes interesadas del sector y otros participantes pertinentes a fin de ayudar a los consumidores a evitar las llamadas y los mensajes de texto automáticos no deseados. Estos temas podrían incluir la notificación al consumidor; si este puede optar por participar, o debe optar por no participar en las herramientas de detección de IA; los mecanismos para la retroalimentación del consumidor; el ajuste de herramientas por parte del consumidor para garantizar la recepción de llamadas y textos.

4. ¿Cómo se utiliza la IA para que las personas con discapacidad puedan hacer llamadas?

Cada vez se utilizan más tecnologías de IA para que las personas con discapacidad puedan hacer llamadas. Entre los ejemplos se encuentran:

- Productos de IA que permiten a las personas con discapacidad motriz realizar llamadas mediante comandos de voz, una función disponible en la mayoría de los teléfonos inteligentes. Los productos modernos de IA también pueden detectar y adaptarse mejor al habla no estándar, ampliando la disponibilidad de las funciones de comandos de voz.
- Servicios de IA que pueden mejorar la detección de movimientos no verbales, como los movimientos oculares y la lengua de señas estadounidense (ASL), permitiendo que estos movimientos controlen interfaces digitales y realicen llamadas.

- *Software* de modelado de voz de texto a voz, el que puede permitir a personas con capacidades de habla limitadas mantener una conversación verbal; algunos productos pueden modelar la voz hablada de una persona. Las medidas para combatir el mercadeo no deseado que se basan en la detección del uso de voz artificial deberían permitir estas conversaciones.
- Las herramientas de IA pueden actuar como voz para alguien que no puede hablar, ya sea por una discapacidad del habla o por una enfermedad debilitante. Esto no solo ayuda a la persona a realizar las tareas cotidianas, sino que puede aumentar sus oportunidades de empleo.

5. ¿Cómo puede la Comisión promover esos usos de conformidad con los requisitos de la Ley de protección al consumidor de servicios telefónicos (Telephone Consumer Protection Act, TCPA) y garantizar que su futura labor contra las llamadas automáticas no los disuada?

Del mismo modo que la Comisión puede promover los usos de la IA para ayudar a los consumidores a evitar telecomunicaciones no deseadas, la FCC puede crear exenciones que abarquen los usos expresamente aprobados de la IA para ayudar a las personas con discapacidad a realizar llamadas y definir las mejores prácticas para estos proveedores de servicios. Esta autoridad se confiere a la Comisión en las siguientes disposiciones del USC: 47 U.S.C. § 227(b)(2)(B), (C)

RECOMENDACIÓN N.º 9: El CAC recomienda a la Comisión adoptar todas las medidas que estén a su alcance para garantizar que su normativa sobre llamadas automáticas no impida el desarrollo y uso de herramientas basadas en IA que permitan a las personas con discapacidad utilizar mejor la red telefónica. Nos complace que la Comisión considere si la legislación vigente le permite eximir dichos usos de la TCPA y la evaluación de posibles cambios a la ley. Además, recomendamos que la Comisión garantice que estas exenciones no sean utilizadas con malas intenciones.

Además, la FCC debería escuchar periódicamente a las personas con discapacidades que utilizan tecnología de asistencia mediante IA y a los programadores informáticos que desarrollan estas herramientas, para garantizar que las actividades de aplicación de normas de la Comisión no obstaculicen involuntariamente las herramientas informáticas. Los medios sociales y otras publicaciones en internet deberían solicitar esta información, pero la FCC también debería intentar proactivamente contactar a personas con discapacidades y a los generadores de dichas herramientas informáticas.

6. ¿Qué actividades de divulgación o educación deben llevarse a cabo para mantener informados a los consumidores sobre el desarrollo de estas tecnologías y aplicaciones?

Para promover el conocimiento y la confianza de los consumidores en los servicios de IA conforme a las normas, la FCC debería crear un sitio web con posibles herramientas de IA y adoptar las medidas mencionadas en los apartados 1 a 3 de este informe. Específicamente, el sitio web debería proporcionar materiales educativos sobre servicios habilitados con IA que puedan 1) ayudar a los consumidores a evitar llamadas y mensajes de texto automáticos no deseados o 2) ayudar a las personas con discapacidades a realizar llamadas o enviar mensajes de texto.

Este registro debe estar alojado en línea, ser de acceso público y ser fácilmente comprensible.

La siguiente sección expone las recomendaciones para una campaña nacional de educación y participación de los consumidores centrada intencionadamente en las estrategias de divulgación a nivel

comunitario y en las asociaciones que la Comisión puede potenciar para maximizar el alcance y la eficacia de esta campaña. El CAC cree que la puesta en práctica de estas recomendaciones puede hacer avanzar el objetivo de preparar y proteger a todos los consumidores frente a las llamadas y mensajes de texto automáticos generados por IA.

RECOMENDACIÓN N.º 10: El CAC recomienda que la Comisión desarrolle esfuerzos nacionales de educación y participación pública en base a una respuesta “3R” para capacitar a los consumidores a fin de que reconozcan, reaccionen y reporten de manera apropiada y segura cuando reciban una llamada o un mensaje de texto automáticos no deseados o maliciosos.

El Comité recomienda que la Comisión emprenda una campaña de educación pública para ayudar a los consumidores a entender cuándo las llamadas y los mensajes de texto automáticos que reciben son generados por IA. Esta campaña debe informar a los consumidores, por lo menos a nivel básico, lo que es la IA y ofrecer casos como ejemplo de uso común para las herramientas potenciadas por la IA. La campaña también debe describir las herramientas de bloqueo de llamadas disponibles o las aplicaciones telefónicas aprobadas por la Comisión que pueden instalarse para detectar e impedir las llamadas y los mensajes de texto automáticos basados en IA.

Esta campaña pública puede seguir un doble enfoque. El primer objetivo es educar a los consumidores sobre los usos emergentes de las tecnologías generadas por IA que repercuten en las llamadas y los mensajes de texto automáticos, así como en cuestiones relacionadas con las telecomunicaciones. En segundo lugar, la campaña podría educar a los consumidores sobre los riesgos y los efectos nocivos de las estafas y los fraudes que suponen las llamadas y los mensajes de texto automáticos generados por IA.

Además, reconociendo que no todas las llamadas y mensajes de texto generados por IA son perjudiciales y que, de hecho, pueden ser beneficiosos, sobre todo para las personas con ciertas discapacidades, una campaña educativa debería destacar los casos de uso positivo de la IA relacionados con los servicios de telecomunicaciones. Para comprender mejor y catalogar esos casos de uso positivo de la IA en las telecomunicaciones, la Comisión debería consultar a grupos vulnerables, grupos de personas con discapacidades, otras agencias federales con competencia interseccional y tecnólogos.

RECOMENDACIÓN N.º 11: El CAC recomienda que la Comisión desarrolle esta campaña y los materiales relacionados con ella en colaboración con organizaciones vinculadas a comunidades desatendidas y de difícil acceso. Esto incluye la creación de contenidos modulares fácilmente adaptables a diferentes idiomas, contextos culturales y perfiles específicos de vulnerabilidad.

A menudo, las campañas de divulgación de “un enfoque para todos” no logran los resultados esperados en los diferentes grupos demográficos ni abordan las vulnerabilidades específicas de los consumidores. Esto deja desatendidos, y más vulnerables a estafas y fraudes, a ciertos grupos demográficos, especialmente a aquellos con barreras lingüísticas o de accesibilidad, a las personas mayores, con discapacidades o ubicadas en contextos culturales diferentes. Para maximizar el alcance y el impacto de las campañas de información, la Comisión podría asociarse con una serie de entidades que atiendan a diversas comunidades con el objetivo de adaptar los mensajes y los métodos de divulgación.

Por ejemplo, la Comisión puede asociarse con organizaciones para:

- Llevar a cabo grupos de sondeo con diversos segmentos demográficos, incluyendo, entre otros, los que se describe a continuación, para garantizar que los mensajes repercutan entre las diferentes comunidades y sean contextual y culturalmente competentes.
- Utilizar una representación diversa en todos los materiales de campaña para

aumentar la identificación y la participación.

- Proporcionar material traducido profesionalmente²¹ a idiomas distintos del inglés, incluyendo, entre otros, los siguientes idiomas en los que la Comisión ya proporciona traducciones:
 - [ÁRABE](#),
 - [CHINO \(TRADICIONAL\)](#),
 - [CHINO \(SIMPLIFICADO\)](#),
 - [FRANCÉS](#),
 - [CRIOLLO HAITIANO](#),
 - [COREANO](#),
 - [PORTUGUÉS](#),
 - [RUSO](#),
 - [ESPAÑOL](#),
 - [TAGALO](#),
 - [VIETNAMITA](#),
 - Lengua de señas estadounidense (ASL).

- Desarrollar descripciones sonoras de todos los materiales visuales, junto con los materiales escritos, para maximizar la accesibilidad de las personas con discapacidad visual.
- Desarrollar versiones simplificadas de todos los materiales para personas con discapacidades cognitivas o alfabetización limitada.
- Incluir contenido y formato en los materiales de campaña que sigan las mejores prácticas para personas mayores, lo que incluye tamaños de letra más grandes, estilos y otras herramientas recomendadas.

Además, la educación de los consumidores y las campañas de divulgación deben ser coherentes y reflejar las realidades vividas por los consumidores. La clave de las campañas duraderas y sostenibles es la creación de materiales y recursos atractivos, adaptables y siempre disponibles que doten a los consumidores de conocimientos y habilidades prácticas para protegerse en un entorno con amenazas en constante evolución. Entre los factores clave que deben tenerse en cuenta a la hora de elaborar materiales y estrategias de implementación de campañas educativas a gran escala que lleguen a los consumidores dondequiera se encuentren podrían figurar los siguientes:

- Dar prioridad a las experiencias de aprendizaje prácticas e interactivas adaptadas a las necesidades específicas y al ritmo del público objetivo.
 - Muchas campañas se centran en distribuir panfletos o en crear sitios web sin garantizar un compromiso activo. A menudo, si la información se dispone de esta manera, no se traduce en cambios de comportamiento ni en desarrollo de habilidades. En su lugar, la Comisión podría desarrollar talleres prácticos, simulaciones y juegos de personificación, con instituciones comunitarias de

²¹ Los materiales deben traducirse utilizando servicios de traducción profesionales que sean lingüística y culturalmente competentes. Si bien las herramientas de IA se utilizan cada vez más para los servicios de traducción, la investigación ha revelado muchas limitaciones clave en su aplicación para este uso. Consulte Nichols and Bhatia, “Lost in Translation: Large Language Models in Non- English Content Analysis” (“Perdido en la traducción: grandes modelos lingüísticos en el análisis de contenido en idiomas distintos al inglés”), Center for Democracy and Technology, 23 de mayo de 2023. <https://cdt.org/insights/lost-in-translation-large-language-models-in-non-english-content-analysis/>

- referencia que permitan a los consumidores practicar la identificación y respuesta a estafas generadas por IA.
- Potenciar el alcance y la participación de los usuarios en plataformas de alta visualización, para ofrecer información oportuna y pertinente.
 - Como cualquier tecnología emergente, la IA está evolucionando rápidamente. Asimismo, las campañas educativas deben ser ágiles y seguir las tendencias del desarrollo tecnológico para estar a la altura de las amenazas que plantea el posible uso indebido de estas tecnologías, sin dejar de reconocer los aspectos y aplicaciones beneficiosos de las mismas.
 - Para mantenerse vigente al ritmo de evolución de las tendencias, la Comisión podría establecer un proceso para actualizar rápidamente los materiales educativos a medida que surjan nuevas herramientas y técnicas de estafas con IA, posiblemente aprovechando la propia IA para ayudar a identificar y analizar nuevas amenazas.
 - Mantener la coherencia de los mensajes a través de múltiples canales para reforzar los aspectos clave mediante la repetición y una presentación variada.
 - Las tecnologías impulsadas por inteligencia artificial y los delincuentes que las utilizan explotan específicamente los sesgos y vulnerabilidades cognitivas. Muchas campañas se centran en la transferencia de conocimientos, sin abordar adecuadamente los factores psicológicos que influyen en los comportamientos de riesgo en línea. Los consumidores pueden comprender los riesgos y, aun así, realizar prácticas inseguras debido a hábitos arraigados o prejuicios cognitivos.
 - Fomentar un sentido de responsabilidad compartida y aprovechar las estructuras comunitarias existentes.
 - Algunas campañas se basan demasiado en tácticas atemorizantes, lo que puede provocar cansancio o falta de compromiso por parte del consumidor. Las campañas deben equilibrar los mensajes preventivos y proactivos con estrategias de capacitación comunitaria que promuevan la resiliencia a nivel de los consumidores y de la comunidad.
 - Al educar sobre los riesgos, los materiales deben enfatizar el poder de una toma de decisiones informada, y recomendar medidas de protección claras y prácticas.
 - Apoyarse en técnicas recreativas para que el aprendizaje sea ameno y competitivo, al tiempo que se fomenta repetidamente el uso de los materiales.

RECOMENDACIÓN N.º 12: El CAC recomienda que la Comisión diseñe un plan de difusión de la campaña multicanal y multimodal para garantizar un amplio alcance y el refuerzo de la campaña educativa. La Comisión debería desarrollar un plan de difusión de la campaña, en colaboración con organizaciones vinculadas a comunidades desatendidas y de difícil acceso, para maximizar el alcance, la accesibilidad y la efectividad de la campaña.

La fuerza de una campaña de educación del consumidor depende de la estrategia de difusión que la haga operativa. Al igual que los principios recomendados anteriormente para crear materiales de campaña inclusivos y accesibles, es fundamental que la Comisión diseñe una estrategia de aplicación de la campaña utilizando diversos medios de comunicación. Al hacerlo, se genera credibilidad y difusión y se facilita el aprendizaje de refuerzo para los consumidores, una vez que estos reciben el contenido y los mensajes mediante varios canales. Esto también garantiza que los consumidores de bajos recursos y limitado acceso a los medios puedan recibir los materiales de la campaña. Entre las tácticas de difusión que la Comisión podría considerar para poner en marcha una campaña de educación, figuran las siguientes:

➤ *Revistas y diarios impresos, y publicaciones en plataformas de la web*

En su estrategia de comunicación, la Comisión podría incluir medios de comunicación impresos tradicionales, así como medios de comunicación que publican solo en internet. De esta forma, garantizaría una amplia audiencia. Dado que los consumidores tienden a confiar en los medios que leen habitualmente, el uso de estos medios también aumentaría la credibilidad de los mensajes. Entre las tácticas que la Comisión podría utilizar, figuran las siguientes:

- Publicar artículos especiales sobre estafas generadas por IA y estrategias de protección en periódicos nacionales y publicaciones²² presentes solo en internet.
- Elaboración de contenidos localizados, para periódicos regionales y locales, destacando las tendencias regionales en materia de estafas y los recursos de apoyo a comunidades, según cada localidad.
- Colocación de carteles informativos y quioscos interactivos en zonas de alto tránsito, como centros comerciales, aeropuertos y centros de transporte público, y en las agencias federales, estatales y locales que prestan servicios directos a los consumidores.
- Crear una columna o boletín periódico con recomendaciones para la seguridad cibernética y alertas de estafas recientes.
 - La Comisión podría colaborar con otras agencias federales que elaboren materiales o boletines relacionados con estafas y fraudes, como la Comisión Federal de Comercio.

➤ *Correo masivo*

Un programa de correo directo de la Comisión permitiría que los mensajes llegaran a los consumidores que posiblemente no tengan acceso a noticias impresas nacionales o locales, y a los consumidores sin acceso digital o con acceso limitado, como quienes integran comunidades rurales. Un programa de correo directo garantizaría que se llegara a los consumidores de comunidades remotas que no puedan acceder a los medios de comunicación tradicionales.

- Grupos demográficos objetivos clave para este programa podrían ser las comunidades rurales y los usuarios de teléfonos de línea fija o de teléfonos celulares del tipo “pago por uso” (pay-as-you-go, en inglés).
 - Es fundamental garantizar que haya un número de teléfono exclusivo

²² Entre los medios que solo publican en internet, figuran proveedores de noticias como Axios.

disponible para que estos consumidores puedan recibir más información, una vez que reciben un correo.

- El nombre, el número de teléfono, la página web y el correo electrónico de la Comisión deben figurar claramente en la correspondencia y en todos los materiales, para mantener la credibilidad y legitimar la información entregada.
- Las organizaciones establecidas en comunidades también pueden ayudar a distribuir folletos de una página, ejemplares de correspondencia y materiales afines.
 - Asociarse con organizaciones comunitarias en la distribución por correo puede consolidar aún más la credibilidad de los materiales.

➤ *Radio*

La mensajería por radio es una forma de comunicación tradicional que ofrece muchas ventajas. Las emisoras de radio suelen ser una fuente fiable que goza de confianza y lealtad entre audiencias específicas en el caso de los consumidores que carecen de acceso a otros medios de comunicación. Además, muchos radioyentes tienen una relación duradera con los presentadores y personalidades de la radio, lo que aumenta la credibilidad de los mensajes. Los mensajes radiofónicos también pueden ser especialmente efectivos para los consumidores con niveles de alfabetización limitados o que carecen de pleno acceso a internet. Como las estaciones de radio también dirigen sus emisiones a nivel regional, los mensajes pueden adaptarse a determinados grupos demográficos, como los de las emisoras rurales o las que no emiten en idioma inglés. Por último, los mensajes radiofónicos podrían rendir más a menor costo que otras formas de difusión, como la televisión o la prensa escrita. Entre las tácticas de difusión que la Comisión podría utilizar a través de la radio figuran las siguientes:

- Producir segmentos de emisión regular, sobre prevención de estafas relacionadas con la IA, para su distribución en cadenas de radio nacionales.
- Colaborar con conocidos locutores o presentadores de radio locales para que compartan consejos de prevención de estafas en sus programas, entre ellos los programas de radio culturales y en otros idiomas, así como los de LGBTQ+ y los programas religiosos.
- Organizar programas con llamadas de los radioyentes, quienes podría dirigir preguntas a expertos en seguridad cibernética o líderes comunitarios confiables.

➤ *Podcasts*

Los *podcasts* (emisiones digitales multimedia) ofrecen beneficios similares a la programación de radio, con algunas ventajas adicionales. Dado que se emiten a la carta, los mensajes que en ellos se transmiten pueden permanecer siempre vigentes y ser recibidos con mayor flexibilidad y accesibilidad por los oyentes. Los podcasts también suelen presentarse en entregas, tienden a cubrir temas especializados y tienen un formato más largo que la programación radiofónica. Esto los hace ideales para un involucramiento repetitivo del oyente y para fomentar su fidelización. Además, los podcasts se pueden compartir fácilmente a través de las redes sociales o aplicaciones de mensajería, lo que aumenta su alcance, gracias a la divulgación persona a persona. Por último, muchas plataformas que albergan podcasts ofrecen transcripciones o subtítulos, lo que hace que los contenidos sean accesibles para las personas con discapacidad auditiva. Entre las tácticas de difusión que la

Comisión puede utilizar a través de los podcasts figuran las siguientes:

- Lanzar una serie de podcasts semanales dedicados a las estafas de IA, e impartiendo conocimientos sobre los medios digitales y la seguridad cibernética.
- Incluir entrevistas con víctimas de estafas, representantes de las fuerzas de orden y expertos en seguridad cibernética y tecnología.
- Colaborar con podcasts que gocen de popularidad y versen sobre tecnología, crímenes reales y protección del consumidor, para llegar a audiencias diversas.
- Colaborar con podcasts étnicos y dirigidos a hablantes de idiomas distintos al inglés, podcasts religiosos y podcasts LGBTQ+.

➤ *Televisión*

La televisión es otro medio de comunicación tradicional que ofrece muchas ventajas. Los segmentos de noticias televisadas y los anuncios de utilidad pública (Public Service Announcements, PSA) pueden otorgar credibilidad y urgencia al mensaje de una campaña y llegar a personas que tal vez no buscarían activamente esta información a través de otros canales. Para los adultos mayores, que pueden estar menos involucrados con los medios digitales, pero son más vulnerables a ciertas estafas, la televisión sigue siendo una fuente de información primaria y confiable. Los mensajes de televisión también ofrecen subtítulos para personas sordas con dificultades auditivas y para quienes no hablan inglés. Al integrar a la televisión en el conjunto más amplio de medios de comunicación, una campaña puede garantizar una cobertura completa y reforzar su mensaje a través de múltiples puntos de contacto, maximizando la eficacia en general y la difusión al público.

Entre las tácticas de difusión que la Comisión podría utilizar a través de la televisión se incluyen:

- Producción de programación especial en horario de máxima audiencia en cadenas nacionales, abordando la evolución de la IA, las estafas y su impacto social.
- Creación de segmentos cortos e informativos para programas matutinos y transmisiones de noticias en estaciones locales, entre ellas los canales en idiomas distintos del inglés.
- Desarrollo de anuncios de utilidad pública (PSA) para su emisión en los períodos de mayor audiencia.
- Presentación de expertos locales en seguridad cibernética y víctimas de crímenes cibernéticos en segmentos informativos de emisoras locales.
- Colocación de PSA en canales de habla no inglesa y en canales culturales especializados.

➤ *Redes sociales*

Las plataformas sociales permiten la difusión de información, dirigida y en tiempo real, sobre estafas emergentes generadas por IA, lo que permite una respuesta rápida a nuevas amenazas. La naturaleza interactiva de las redes sociales facilita la comunicación recíproca, permitiendo a la Comisión abordar directamente las preocupaciones del público y recabar comentarios. Además, la capacidad de difusión de las redes sociales puede amplificar el mensaje de la campaña a través de las redes que facilitan la comunicación entre pares, aumentando su confianza y credibilidad. Las tácticas de difusión en redes sociales que la Comisión podría utilizar incluyen:

- Aprovechar funciones específicas de la plataforma, como los videos breves, las infografías y las sesiones de preguntas y respuestas en directo, para ofrecer contenidos en formatos diversos y atractivos que resuenen en distintos segmentos de audiencia.
- Utilizar la segmentación demográfica adecuada y respetuosa con los derechos que ofrecen las plataformas de medios sociales para llegar a comunidades individualizadas con mensajes cultural y contextualmente apropiados.
- Colaborar con creadores, influyentes culturales y voces de confianza de la comunidad para fomentar la participación de los consumidores y llegar a ellos en espacios culturales no tradicionales.

➤ *Eventos en persona*

Una estrategia de participación en persona sigue siendo crucial para las campañas de educación e información, ya que fomenta conexiones directas y significativas con los consumidores. Las interacciones personales generan confianza y credibilidad y permiten debates matizados y una retroalimentación inmediata que los medios digitales o de difusión no pueden replicar. Esta participación personal brinda la oportunidad de abordar las preocupaciones locales, adaptar los mensajes a las diversas necesidades de la comunidad y demostrar el compromiso de la Comisión de servir a todos los consumidores. Además, los eventos en persona pueden llegar a grupos demográficos con acceso limitado a canales de comunicación de otro tipo. Al combinar la autenticidad de la interacción humana con el amplio alcance de otras estrategias de medios, un enfoque presencial fortalece el impacto general y la eficacia de la campaña.

La Comisión podría:

- Organizar reuniones en conjunto con autoridades locales de varias comunidades, para abordar el tema de las estafas generadas por la IA y las estrategias de protección, a lo largo del ciclo de vida de la campaña educativa.
- Organizar talleres en bibliotecas locales, centros comunitarios, instituciones religiosas, escuelas y centros de personas mayores y de residentes autodependientes, en los que se ofrezcan demostraciones prácticas sobre cómo identificar llamadas y mensajes de texto generados por IA.
- Instalar puestos informativos en actos comunitarios, ferias y mercados agrícolas.
- Presentarse en actos organizados por asociaciones del sector de las telecomunicaciones, incluso en colaboración con líderes de la industria.

RECOMENDACIÓN N.º 13: El CAC recomienda que la Comisión establezca y mantenga asociaciones permanentes con instituciones y organizaciones comunitarias de referencia, con fuertes vínculos comunitarios y de bases, en apoyo de una campaña de educación e información.

La continua participación de las partes interesadas con las organizaciones comunitarias puede potenciar las redes de confianza y la experiencia existentes, para llegar eficazmente a comunidades diversas. Estas asociaciones permiten enviar mensajes a medida que tienen resonancia en grupos específicos, entre ellos los que sean especialmente vulnerables a las estafas generadas por la IA. Este enfoque colaborativo fomenta el desarrollo de recursos educativos y soluciones tecnológicas innovadoras, garantizando que la campaña educativa se mantenga a la vanguardia de las amenazas emergentes. Esta estrategia crea una red

sostenible, de defensores de la seguridad digital, impulsada por la comunidad, aumentando el impacto y la longevidad de la campaña. La Comisión también puede convocar a otras partes interesadas, como instituciones educativas, otras agencias u organismos gubernamentales, y socios de la industria. La Comisión podría fomentar asociaciones sólidas y diversas entre las partes interesadas mediante:

- La colaboración con bibliotecas, centros comunitarios, organizaciones comunitarias, centros para personas mayores y de residentes autodependientes, instituciones religiosas e instituciones comunitarias relacionadas, para organizar talleres educativos²³.
- La asociación con organizaciones que trabajan en el punto de encuentro entre aspectos identitarios y tecnológicos, para generar conciencia sobre preocupaciones particulares de las comunidades que podrían ser blanco de estafas.
- La asociación con agencias locales de protección al consumidor para adaptar y ampliar los mensajes y los recursos.
- La maximización de asociaciones con grupos estructurados para involucrar a las comunidades en un espacio de participación cívica, a fin de promover la información sobre cómo las llamadas automáticas mediante IA y los mensajes de texto automáticos pueden utilizarse para influir en las elecciones²⁴.
- El desarrollo de módulos del plan de estudios para escuelas, a fin de enseñar a los estudiantes sobre las estafas generadas por IA e impartir conocimientos sobre los medios digitales, lo que incluye colegios comunitarios y programas de educación para adultos.
- La colaboración con universidades para investigar las nuevas técnicas de estafa con IA y eficaces estrategias de prevención.
- El ofrecimiento de programas de capacitación para que los educadores se conviertan en “embajadores de la seguridad digital” en sus comunidades.
- La colaboración con centros de trabajo y empresas para impartir a los empleados formación sobre estafas con el uso de la IA.
- La creación de guías específicas de la industria sobre cómo las estafas generadas por IA podrían dirigirse a diferentes profesiones.
- El trabajo con los fabricantes de teléfonos inteligentes para desarrollar las mejores prácticas para integrar en los dispositivos funciones de detección de estafas mediante el uso de inteligencia artificial para preservar los derechos intelectuales.
- La colaboración con empresas de IA para desarrollar y aplicar normas éticas relacionadas con la clonación de voz y otras tecnologías de IA.

RECOMENDACIÓN N.º 14: El CAC recomienda que la Comisión desarrolle un modelo de “entrenamiento para capacitadores” destinado a aumentar la capacidad y la resistencia de la comunidad, para responder de forma segura y adecuada a las llamadas y mensajes de texto automáticos.

Una vez que los materiales educativos y de campaña se hayan desarrollado y difundido en conjunto con diversas partes interesadas, la Comisión también podría considerar la posibilidad de aumentar la

²³ Incluyendo a centros comunitarios LGBTQ a través de Centerlink, a organizaciones estatales a través de la Equality Federation (“federación para la igualdad”) y a centros de personas mayores a través de Services and Advocacy for Gay, Lesbian, Bisexual, and Transgender Elders (“servicios y defensa de los adultos mayores gays, lesbianas, bisexuales y transexuales”, SAGE, por sus siglas en inglés).

²⁴ Estos grupos podrían incluir, por ejemplo, el LGBT Equality Caucus o el Victory Fund Institute y grupos similares.

capacidad de respuesta de la comunidad mediante el diseño de un programa de “entrenamiento para capacitadores” que prepare a los consumidores para educarse mutuamente sobre los riesgos que plantean las llamadas y mensajes de texto automáticos habilitados con IA. El aprendizaje entre pares ofrece muchas ventajas y maximiza el alcance y la escala de una campaña de educación básica, al añadir una nueva dimensión y matices culturales y regionales a los materiales educativos distribuidos.

Al establecer un modelo de entrenamiento para capacitadores, también se proporciona un marco estructurado a través del cual la Comisión puede añadir materiales nuevos o actualizados, entre ellos temas multidisciplinarios, como conocimientos sobre banda ancha y otros que sean de prioridad para los consumidores. Estos modelos también pueden servir para informar a la Comisión sobre nuevas tendencias de fraude o nuevos usos de las herramientas de IA usados por estafadores para explotar a los consumidores. Como parte de un programa de “entrenamiento para capacitadores”, la Comisión podría desarrollar:

➤ *Un plan de capacitación integral*

- La Comisión podría desarrollar un plan de estudios modular que cubra la tecnología de la IA, la identificación de estafas y estrategias de protección, y que se adapte, en general, a los materiales de educación desarrollados en la recomendación anterior.
- La Comisión podría crear presentaciones en diapositivas, materiales didácticos y ejercicios interactivos para los capacitadores. Estos materiales podrían utilizarse en la campaña informativa y educacional, además de otros materiales desarrollados específicamente para este modelo.
- La Comisión podría trabajar con instituciones comunitarias para brindar orientación sobre cómo adaptar los materiales para diferentes públicos (por ejemplo, personas mayores, jóvenes, la comunidad de discapacitados y hablantes cuya lengua materna no sea el inglés).

➤ *Una plataforma de aprendizaje en línea*

- La Comisión podría establecer un centro de recursos en línea al que los capacitadores puedan acceder y compartir materiales de capacitación, mejores prácticas, estudios de casos y otros recursos relevantes. Este centro podría ser una plataforma de aprendizaje continuo para capacitadores y sus estudiantes, así como un mecanismo para que la Comisión recopile información sobre las tendencias relacionadas con las llamadas automáticas y los mensajes de texto automáticos generados por IA.
 - Este eje centralizado puede incluir un foro para que los capacitadores compartan experiencias y buenas prácticas. La Comisión debería revisar periódicamente estos foros o reunirse con los capacitadores, para informarles sobre las mejores prácticas en evolución e identificar nuevas necesidades de la comunidad o de los consumidores.
- La Comisión podría ofrecer seminarios web y módulos de capacitación virtual, para el desarrollo continuo de los capacitadores.

➤ *Un programa de colaboración con organizaciones comunitarias*

- La Comisión podría establecer formalmente acuerdos de colaboración con diversas organizaciones comunitarias, como centros de adultos mayores, centros de residentes autodependientes, bibliotecas, colegios comunitarios, instituciones religiosas, organizaciones culturales y organizaciones confesionales, para promover el modelo de entrenamiento de capacitadores y reclutar capacitadores y estudiantes.
- La Comisión podría conceder subvenciones o remuneraciones a organizaciones comunitarias para que pongan en marcha programas de educación sobre las estafas que usan IA.
- También se podría ofrecer apoyo técnico y recursos a las organizaciones comunitarias, para la aplicación del programa.

➤ *Un circuito de retroalimentación y mejoras*

- La Comisión podría llevar a cabo encuestas periódicas y grupos de discusión con capacitadores y estudiantes, para conocer su opinión sobre el programa, e identificar las nuevas amenazas que plantea el uso de la IA en relación con las llamadas y mensajes de texto automáticos.
- La Comisión podría analizar los datos sobre denuncias de estafas y los índices de éxito del modelo de prevención, para perfeccionar los materiales de capacitación.
- También se podrían organizar reuniones de capacitadores y partes interesadas para compartir ideas, actualizar estrategias y perfeccionar las mejores prácticas.

RECOMENDACIÓN N.º 15: El CAC recomienda que la Comisión incorpore una campaña de educación sobre llamadas y mensajes de texto automáticos, generados por IA, con iniciativas de acceso a la banda ancha y entrenamiento en el ámbito digital.

La falta de exposición y participación en el ámbito de las tecnologías emergentes como la IA es una extensión de la brecha digital. La Comisión debería aprovechar las iniciativas existentes de acceso a la banda ancha y de entrenamiento en materia digital²⁵ y las herramientas para llegar a los consumidores más vulnerables a las estafas y los fraudes generados por IA. La combinación de estos temas puede ampliar el alcance de estas comunicaciones y potenciar la credibilidad existente asociada con estas campañas para consolidar aún más la interacción del consumidor con los materiales. Esta estrategia puede ser especialmente útil para llegar a las comunidades históricamente sobrerrepresentadas en la brecha digital, que también pueden estar menos informadas de los riesgos asociados a las llamadas y los mensajes de texto automáticos.

RECOMENDACIÓN N.º 16: El CAC recomienda que la Comisión amplíe su Centro para consultas y quejas de los consumidores (Consumer Inquiries and Complaints Center).

La ampliación y mejora del Centro de la FCC para consultas y quejas de los consumidores (Consumer

²⁵ Las iniciativas a impulsar pueden incluir la iniciativa Homework Gap and Connectivity Divide (“brecha de tareas escolares y la conectividad”), el Rural Broadband Accountability Plan (“plan de responsabilidad de banda ancha rural”) o la iniciativa Broadband Data Collection (“recopilación de datos de banda ancha”), todas ellas llevadas a cabo por la Comisión.

Inquiries and Complaints Center) es fundamental para combatir eficazmente las estafas generadas por IA y proteger a los consumidores. Al mejorar la visibilidad, agilizar los procesos y potenciar la tecnología, el Centro puede convertirse en un recurso más accesible y receptivo para el consumidor. Este planteamiento permite a los consumidores notificar problemas rápidamente y a la Comisión recopilar datos sobre amenazas emergentes, útiles a la hora de fundamentar medidas proactivas y decisiones políticas. Además, las mejoras propuestas, entre ellas el soporte multilingüe y estudios demográficos exhaustivos, garantizan que el Centro pueda atender a diversas comunidades de manera equitativa, convirtiéndolo en una herramienta indispensable en la lucha contra el fraude digital. Algunas de las medidas que puede adoptar la Comisión son:

- *Mejorar la notoriedad del Centro de la FCC para consultas y quejas de los consumidores (Consumer Inquiries and Complaints Center)*
 - Integrar y vincular al Centro para el consumidor en todos los materiales educativos y de mensajería.
 - Colaborar con empresas de telecomunicaciones y asociaciones de la industria, para incluir información sobre el Centro en las comunicaciones con clientes y miembros.
 - Desarrollar una aplicación móvil para acceder fácilmente a los recursos del Centro y al sistema de presentación de quejas.

- *Agilizar el proceso de quejas de la Comisión*
 - Simplificar el formulario de denuncia en línea, facilitando su uso y accesibilidad para las personas con conocimientos limitados de inglés, y en diversos dispositivos y medios.
 - Adoptar “chatbots” (chateo automatizado) utilizando IA, para guiar a los usuarios a través del proceso de quejas y para dar respuestas instantáneas a consultas comunes. Al utilizar los “chatbots”, será necesario advertir a los consumidores que se están comunicando con un robot, dándoles la opción de evitarlos (“opt-out”).
 - Establecer una línea directa dedicada a recibir denuncias sobre llamadas y mensajes de texto fraudulentos generados por IA.

- *Mejorar los tiempos de respuesta y los procedimientos de seguimiento de la Comisión*
 - Aumentar el personal y los recursos dedicados a gestionar el creciente volumen de quejas relacionadas con la IA.
 - Aplicar un sistema de seguimiento automatizado para mantener informados a los consumidores sobre el estado de sus quejas.
 - Crear un equipo de respuesta rápida para gestionar las denuncias de estafas generadas por IA.
 - Supervisar periódicamente las quejas, para identificar oportunamente los temas a abordar en los materiales educativos y campañas de divulgación y educación.

➤ *Estudio demográfico exhaustivo*

- Llevar a cabo investigaciones a escala nacional para identificar patrones de victimización en función de la edad, los ingresos, la educación y la ubicación geográfica.
- Analizar los datos de las estafas denunciadas, para identificar vulnerabilidades o temas utilizados más comúnmente por los estafadores.

APÉNDICE

Miembros del CAC de la FCC de 2024

- Funcionaria federal designada: **Keyla Hernandez-Ulloa**, jefa asociada, división de divulgación para asuntos del consumidor, Oficina de Asuntos Gubernamentales y del Consumidor (Consumer and Governmental Affairs Bureau, CGB, por sus siglas en inglés), Comisión Federal de Comunicaciones.
- Funcionario federal designado adjunto: **David M. Pérez**, director nacional de impacto comunitario, CGB, Comisión Federal de Comunicaciones.
- Exfuncionaria federal designada: **Cara Grayer**, abogada asesora, división de políticas al consumidor, CGB, Comisión Federal de Comunicaciones.
- Exfuncionaria federal designada, **Diana Coho**, especialista en asuntos del consumidor y divulgación, división de divulgación para asuntos del consumidor, CGB, Comisión Federal de Comunicaciones.

- Copresidenta del CAC: UnidosUS, **Claudia Ruiz**, analista de Derechos Civiles.
- Copresidenta del CAC: Copresidente del CAC: Liga Nacional de Consumidores, **John Breyault**, vicepresidente de Políticas Públicas, Telecomunicaciones y Fraude.
 - (Suplente) **Eden Iscil**, gerente de Políticas Públicas.
- Asociación Estadounidense de Personas Jubiladas (American Association of Retired Persons, AARP), **Dawit Kahsai**, directora de Asuntos Gubernamentales.
 - (Suplente) **Coralette Hannon**, directora de Comunidades Habitables / Asuntos Gubernamentales.
- Asociación estadounidense del cable (American Cable Association, ACA Connects), **Brian Hurley**, asesor principal de Reglamentación.
 - (Suplente) **Bill Tortoriello**, director de Asuntos Reglamentarios.
- Asian-Americans Advancing Justice (AAJC), **John Yang**, presidente y director ejecutivo.
 - (Suplente) **Nicole Morgenstern**, gerente asociada de Políticas de Telecomunicaciones, Tecnología y Medios.
- AT&T, **Linda Vandeloop**, vicepresidenta adjunta, Asuntos externos / Reglamentación.
 - (Suplente) **Angela DeMahy**, directora de Asuntos Reglamentarios Federales y Legislativos Externos.
- *Individualmente*, **Cody Dorsey**, director ejecutivo, Baltimore Digital Equity Coalition (Coalición de Equidad Digital de Baltimore).
- Common Sense Media, **Amina Fazlullah**, directora sénior de Política de Equidad.
- Consumer Technology Association (Asociación de Tecnología del Consumidor), **Rachel Sanford Nemeth**, directora sénior de Asuntos Reglamentarios.
 - (Suplente) **David Grossman**, vicepresidente de Asuntos Reglamentarios.
- Deep East Texas Council of Governments (Consejo de Gobiernos del Este Profundo de Texas), **Mickey M. Slimp**, asesor de proyectos de banda ancha.

- (Suplente) **Robert Bashaw**, oficial de Información Pública, Planificador Regional.
- INCOMPAS, **Lindsay Stern**, abogada y asesora de políticas.
 - (Suplente) **Christopher Shipley**, director ejecutivo de Políticas Públicas.
- Consejo de la Industria de la Tecnología de la Información (Information Technology Industry Council, ITI), **Katherine (Katie) McAuliffe**, directora de Política de Telecomunicaciones.
- The Kapor Center, **Lili Gangas**, directora de la Comunidad Tecnológica.
- LGBT Technology Institute (Instituto Tecnológico LGBT), **Kristen Kelley**, directora de Programas.
 - (Suplente) **Ellie Besette**, directora de Operaciones y Finanzas.
- Departamento de Telecomunicaciones y Cable de Massachusetts, **Joslyn Day**, directora, División de Consumidores.
 - (Suplente) **William Bendetson**, presidente de la División Legal.
- Consejo Multicultural de Medios de Comunicación, Telecomunicaciones e Internet, **Kenley Joseph**, asesor de Política Tecnológica y de Telecomunicaciones.
 - (Suplente) **Robert Branson**, presidente y director general.
- Asociación Nacional de Radiodifusores (National Association of Broadcasters NAB), **Liliana Rañón**, vicepresidenta de Asuntos Exteriores.
 - (Suplente) **Larry Walke**, consejero General Adjunto.
- Asociación Nacional de Funcionarios y Asesores de Telecomunicaciones (National Association of Telecommunications Officers and Advisors, NATOA), **Mitsuko Herrera**, Planificación, Política y Proyectos Especiales del Condado de Montgomery, Maryland.
 - (Suplente) **Frederick Ellrod III**, director de la División de Política y Reglamentación de las Comunicaciones.
- Centro Nacional de Derechos del Consumidor (National Consumer Law Center, NCLC), **Olivia Wein**, abogada sénior.
 - (Suplente) **Margot Saunders**, abogada sénior.
- National Diversity Coalition (Coalición Nacional para la Diversidad), **Faith Bautista**, directora General y presidenta.
- Next Century Cities, **Andrew Stutzman**, director ejecutivo.
 - (Suplente) **Ryan Johnston**, asesor político sénior.
- Northern Virginia Urban League, Inc. (Liga Urbana del Norte de Virginia, Inc.), **Scott Alfred Price**, miembro del Consejo de Administración.
- Proyecto GOAL, **Debra Berlyn**, directora ejecutiva.
- RuralRISE / Centro Nacional para el Desarrollo de la Investigación (National Center for Research Development, NCRD), **Tina Metzner**, vicepresidenta y cofundadora.
- (Suplente) **Joseph Kapp**, presidente y cofundador.
- TDI for Access, Inc., **AnnMarie Killian**, directora ejecutiva.
- The Hispanic Federation (La Federación Hispana), **Brent Wilkes**, vicepresidente sénior de Desarrollo Institucional.
- Asociación de Internet y Televisión (The Internet & Television Association, NCTA), **Radhika Bhat**, vicepresidenta y asesora general adjunta.
 - (Suplente) **Steven Morris**, vicepresidente y asesor general adjunto.
- The Trevor Project, **Kasey Suffredini**, vicepresidenta sénior interina de Prevención.
 - (Suplente) **Casey Pick**, director de Derecho y Políticas.
- Asociación de Telecomunicaciones de Estados Unidos (United States Telecom Association [USTelecom]), **Diana Eisner**, vicepresidenta de Políticas y Defensa.
 - (Suplente) **Josh Bercu**, vicepresidente de Política y Promoción.