Before the
NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION
U.S. DEPARTMENT OF COMMERCE
Washington, D.C. 20230

	)	
AI Accountability Policy Request for Comment	**)**	NTIA Docket No. 230407-0093
	)	

COMMENTS OF
NCTA—THE INTERNET & TELEVISION ASSOCIATION

Rick Chessen
Loretta Polk
Traci Biswese
NCTA – The Internet &
Television Association
25 Massachusetts Avenue NW
Suite 100
Washington, DC 20001
(202) 222-2445

June 12, 2023

TABLE OF CONTENTS

INTRODUCTION

NCTA – The Internet & Television Association (NCTA) welcomes the opportunity to participate in NTIA's examination of Artificial Intelligence ("AI") system accountability measures and policies.[1] This proceeding can be used to explore both positive and potentially harmful applications of AI. The challenge is finding effective ways to promote AI trust, accountability, and fairness, and thereby maximize potential consumer benefits and minimize potential risks. As described below, we believe NTIA should take a measured, multi-stakeholder approach to AI accountability that is based on risk and likelihood of harm.

I.   NCTA MEMBERS ARE RESPONSIBLY USING AI TECHNOLOGIES.

Current technological AI innovations within the cable industry are diverse and touch upon many areas of the business for network operations/security, content customization, enhanced service offerings, customer experiences, and fraud prevention. Operational benefits and use cases include:

- o   Decreasing service downtime through proactive and reactive network maintenance, network resilience, and data analytics.

- o   Ensuring security of broadband networks and end user accounts through enhanced network security and cyber security detection tools.

---

[1] NCTA member companies operate some of the largest and most advanced broadband networks in the world, providing cutting-edge video, voice, and data services to consumers nationwide. Our members are also some of the nation's leading creators of content that entertains, informs, and inspires millions of consumers in the US and around the globe. We therefore have a significant interest in the range of issues raised in the Request for Comment.

o   Enabling content creators to enhance the viewer experience, making visual effects more dramatic, realistic, and enjoyable.

o   Improved consumer accessibility and optionality via recommendation engines for programming, voice remotes, and text-to-speech.

o   Support for virtual, anytime customer service, online sales and onboarding, and home security products.

Accessibility is a particularly promising use case for AI. The cable industry has consistently served as a leader in advancing accessibility, including a long history of collaboration with disability communities to improve user experience.[2] For instance, NCTA members are researching and investing in automatic speech recognition ("ASR") which, when coupled with appropriate quality controls, has the potential to drastically reduce captioning errors and improve caption synchronicity and completeness. ASR and other technologies based on machine learning offer particularly exciting solutions because the output of the solutions improves the longer and more widely the products are in use.[3] We look forward to considering how such technologies can improve the user experience in consultation with advocates for people with disabilities.

Another innovative AI use case is proactive network maintenance. Comcast, for instance, successfully used AI and Machine Learning (ML) during the COVID-19 pandemic to identify

---

[2] *See, e.g.*, Comments of NCTA – The Internet & Television Association, MB Docket No. 12-108 (filed Mar. 03, 2023).

[3] Comments of NCTA – The Internet & Television Association, GN Docket No. 21-140, at 7-8 (filed June 7, 2021. *See also* Reply Comments of The National Association of Broadcasters, CG Docket No. 05-231, at 5 (filed Oct. 30, 2019) (explaining that "ASR is still a relatively new technique, but has started to show some promise that it could play a useful role in ensuring accessibility to video programming. NCTA notes that some of its members have rolled out ASR on some networks and found that ASR can produce more complete live captions than human captioners. Given that ASR is based on artificial intelligence and machine learning, it is also more likely to continue to improve than human captioning.").

areas where network capacity should be increased even before customers experienced congestion.[4]

As even more advanced networks such as cable's 10G networks are built out,[5] there will be a

growing need to further automate additional network management and operations tasks using AI

technologies. These applications of AI are targeted towards improving existing business processes

that lower cost while increasing service quality.

II.   FRAMEWORK FOR AI ACCOUNTABILITY

A. A Risk-Based Framework is the Best Approach to Balancing the Competing Considerations Associated with AI Accountability.

Risk management is fundamentally a balancing test that involves identifying benefits,

fostering awareness of potential harms and their severity, prioritizing actions, incorporating

applicable legal and regulatory obligations, mitigating known risks, and assessing and refining an

organization's privacy risk management practices.[6] Risk not only varies by AI use case but can

change throughout the lifecycles of each AI use case – which include design, development,

---

[4] *COVID-19 Network Report: How A Smart Network Delivered Speed and Stability When it Mattered,* Comcast.com (July 13, 2020), https://corporate.comcast.com/stories/covid-19-network-report-smart-network-speed-and-stability. Comcast Octave is an AI-based platform, developed by Comcast engineers in Philadelphia that checks 4,000+ telemetry data points (such as external network "noise", power levels, and other technical issues that can add up to a big impact on performance) on tens of millions of modems across our network every 20 minutes. The Octave system was able to create 36% more usable capacity through AI alone, enabling the company to "optimize the network at the speed of software". ML-based platforms include those that dramatically reduce the time to identify and fix network impairments or even to improve issues before customers notice.

[5] 10G is the broadband platform of the future that will deliver improved capacity and reliability, lower latency, and faster speeds across a broad population of customers, not just the select few at the end of some companies' individual fiber builds. With upgraded power and capacity, 10G will enable creators and innovators to fulfill their dreams while providing reliability and security. *See* NCTA, *The Future is 10G*, https://www.ncta.com/positions/the-future-of-superfast-internet (last visited May 17, 2023).

[6] NCTA – The Internet & Television Association Comments on the Federal Trade Commission's Commercial Surveillance and Data Security Rulemaking, R111004 (filed Nov. 21, 2022), https://www.regulations.gov/comment/FTC-2022-0053-1097 (*NCTA FTC Comments*).

deployment, and post-deployment. Accordingly, it is incumbent on stakeholders to monitor their

AI systems at all stages of the lifecycle with processes to identify, mitigate, and track risk.[7]

The AI Risk Management Framework[8] produced by the National Institute of Standards

and Technology (NIST) is a flexible and adaptable resource for organizations to think about and

manage risk. Risk management does not seek to eliminate all potential risks or prevent all

possible harms. It is instead focused on identifying and prioritizing risks so that they can be

addressed in a way that is context specific and proportionate with potential corresponding harms

to consumers. Because there is a continuum of risks associated with different types of AI system

use cases, which may include consumer data collection, use, and disclosure practices, NTIA

should consider the prevalence of a practice, the magnitude of the risk posed by the practice and

the data at issue, as well as benefits that the practice will enable.[9]

B. An AI Accountability Framework Should Consider Risk-Based Frameworks in Other Subject Areas

Privacy. NCTA supports enactment of comprehensive privacy legislation that contains

provisions designed to deter and remedy data use practices and actions by online providers that

---

[7] One example of a risk management process that Comcast uses is Privacy Impact Assessment (PIA). *See* Federal Trade Commission, *Privacy Impact Assessments*, https://www.ftc.gov/policy-notices/privacy-policy/privacy-impact-assessments (last visited on May 30, 2023) (defining the term as "an analysis of how personally identifiable information is collected, used, shared, and maintained. The purpose of a PIA is to demonstrate that program managers and system owners at the FTC have consciously incorporated privacy protections throughout the development life cycle of a system or program.") Comcast also uses System Development Lifecycle (SDL). *See* Comcast, *Comcast's Secure Development Lifecycle (SDL): Building In Stronger Cybersecurity End-to-End*, https://corporate.comcast.com/stories/comcast-secure-development-lifecycle-stronger-cybersecurity-end-to-end (last visited on May 30, 2023) (defining "SDL" as "an end-to-end approach designed to deliver highly secure products, whether devices, networks, systems, APIs or services, from concept to end of life.").

[8] National Institute for Standards and Technology, *Artificial Intelligence Risk Management Framework 1.0* (Jan. 2023), https://nvlpubs.nist.gov/nistpubs/ai/ NIST.AI.100-1.pdf.

[9] *NCTA FTC Comments* at 18.

result in civil rights violations.[10] A national privacy framework would address privacy-related

harms from AI systems, and should encourage a risk-based approach that directs organizations to

mitigate the risk of harmful uses or unwanted exposure of consumers' personal data while

providing flexibility to encourage innovation in data usage and protection practices and privacy

tools. NTIA's study of AI Accountability should examine and adapt the most salient aspects of

that approach here.[11]

        Cybersecurity. As the nation's largest providers of broadband Internet access service,[12]

NCTA's members work every day to detect, prevent, and mitigate cybersecurity threats of all

forms to minimize their impact on broadband networks and consumers. The cable industry has a

long history of providing its customers with the benefits of secure networks, including by

employing key secure routing tools and protocols, like Resource Public Key Infrastructure

(RPKI),[13] investing in cutting edge security for the equipment companies issue to consumers,

promoting secure equipment authentication and identity best practices through industry standards

and NIST guidance, maintaining routine communication with government stakeholders to help

---

[10] Letter Response of NCTA – The Internet & Television Association, Docket No. NTIA-2023-0001 – Privacy, Equity, and Civil Rights Request for Comment at 1 (Filed Mar. 6, 2023). Comprehensive privacy legislation would address some of the harms that could stem from the use of AI, but privacy is not an appropriate vehicle to address all potential AI harms.

[11] *NCTA FTC Comments* at 5-6.

[12] In addition to its commitment to accountability, NCTA and its members have long shared NTIA's and the FCC's commitment to ensuring that all Americans have robust broadband internet access service available. Cable providers are at the forefront of advancing the goals of universal access and connecting American consumers and have been leaders in providing affordable options for low-income consumers.

[13] Oliver Borchert et al., *BGP Secure Routing Extension (BGP-SRX): Reference Implementation and Test Tools for Emerging BGP Security Standards*, NIST Technical Note 2060 (2021), https://nvlpubs.nist.gov/nistpubs/TechnicalNotes/NIST.TN.2060.pdf.

respond to, anticipate, and mitigate cybersecurity incidents, and through the industry's support of other critical cybersecurity initiatives.[14]

The federal government has sought to leverage the dynamism of varying approaches to cybersecurity by promoting a risk management model to improve the nation's cyber defense posture. This approach fosters accountability and flexibility to allow companies to assess and take measures best suited to address and mitigate the variety of unique and constantly evolving cybersecurity risks they face.[15] By building on the foundational risk management model developed in collaboration with industry for cybersecurity, NIST has initiated important work on applying risk-management principles to aid organizations in identifying, evaluating, prioritizing, and responding to privacy risks.[16] NIST has furthered this work through its AI Risk Management Framework which serves as a "resource to organizations designing, developing, deploying, or using AI systems to help manage" risks and promote responsible and trustworthy AI design and use.[17] NCTA encourages NTIA and other federal stakeholders to work closely with NIST

---

[14] The cable industry has been deeply involved in the development of the National Institute of Standards and Technology (NIST) Cybersecurity Framework and Internet of Things (IoT) device security standards forged via multi-stakeholder processes at NIST and NTIA. *See, e.g.*, Comments of NCTA – The Internet & Television Association, PS Docket No. 22-90 (filed Apr. 11, 2022). *See, e.g.*, Managed Security — Comcast Business, Masergy, https://www.masergy.com/managed-security (last visited May 30, 2023).

[15] *See* National Institute for Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity* (Apr. 16, 2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf ("The Framework enables organizations – regardless of size, degree of cybersecurity risk, or cybersecurity sophistication – to apply the principles and best practices of risk management to improving security and resilience.").

[16] *See* National Institute for Standards and Technology, *NIST Privacy Framework: A Tool for Improving Enterprise Privacy Risk Management* (Preliminary Draft Sept. 6, 2019).

[17] *See* National Institute for Standards and Technology, *Artificial Intelligence Risk Management Framework (AI RMF 1.0)* (Jan. 2023), at 1 (explaining that, "[l]ike risks for other types of technology, AI risks can emerge in a variety of ways and can be characterized as long- or short-term, high- or low-probability, systemic or localized, and high- or low-impact.").

through a risk-management lens, as it moves forward in its study and report on AI

Accountability.[18]

      Fraud Prevention. NCTA member companies dedicate significant resources to combat

impersonation fraud in its many forms and work diligently to identify and stop scammers, assist

law enforcement agencies, educate consumers and businesses about common scams and fraud

prevention, and undertake extensive technological mitigation efforts.[19] These efforts will

continue as NCTA's member companies explore and deploy advanced digital technologies such

as AI.

---

[18] *See, e.g., OECD, Recommendation of the Council on OECD Legal Instruments Artificial Intelligence* (Adopted May 21, 2019), available at https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449 ("The Recommendation aims to foster innovation and trust in AI by promoting the responsible stewardship of trustworthy AI while ensuring respect for human rights and democratic values."); United Nations, *Guiding Principles on Business and Human Rights* (2011), available at https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf ("These Guiding Principles should be understood as a coherent whole and should be read, individually and collectively, in terms of their objective of enhancing standards and practices with regard to business and human rights so as to achieve tangible results for affected individuals and communities, and thereby also contributing to a socially sustainable globalization;" and "States also have the duty to protect and promote the rule of law, including by taking measures to ensure equality before the law, fairness in its application, and by providing for adequate accountability, legal certainty, and procedural and legal transparency.").

[19] *See, e.g.*, NCTA– The Internet & Television Association Comments on the Federal Trade Commission's Impersonation Rulemaking, R207000 (filed. 16, 2022).

CONCLUSION

NCTA looks forward to working with NTIA and other stakeholders to promote AI

accountability and the other important issues in this proceeding.

Respectfully submitted,

/s/ Rick Chessen

Rick Chessen
Loretta Polk
Traci Biswese
NCTA – The Internet &
Television Association
25 Massachusetts Avenue NW
Suite 100
Washington, DC 20001
(202) 222-2445

June 12, 2023