Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Access to Video Conferencing	)	CG Docket No. 23-161
	)	
Implementation of Sections 716 and 717 of the Communications Act of 1934, as Enacted by the Twenty-First Century Communications and Video Accessibility Act of 2010	)	CG Docket No. 10-213
	)	
Telecommunications Relay Services and Speech-to-Speech Services for Individuals with Hearing and Speech Disabilities	)	CG Docket No. 03-123
	)	
Petition of Sorenson Communications, LLC for a Limited Waiver of the Privacy Screen Rule	)	

COMMENTS ON NOTICE OF PROPOSED RULEMAKING

by

Electronic Privacy Information Center (EPIC)

Submitted September 6, 2023

Chris Frascella
Counsel
Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036

Jake Wiener
Counsel
Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036

Comments

I. Introduction

The Electronic Privacy Information Center (EPIC) files these comments to provide feedback and applaud the Federal Communications Commission ("Commission" or "FCC") for its attention to privacy, accessibility, and interoperability concerns with telecommunications relay services (TRS) on video conferencing platforms.[1] We urge the Commission to be explicit that TRS providers cannot train machine learning sets using live consumer data without express, affirmative consumer consent, and we support the Commission's proposals to clarify that its privacy protections extend to non-relayed content and to automated TRS tools that do not utilize a communications assistant (CA).

EPIC is a public interest research center in Washington, D.C., established in 1994 to secure the fundamental right to privacy in the digital age for all people through advocacy, research, and litigation.[2] EPIC has long defended the rights of consumers and has played a leading role in developing the Commission's authority to address emerging privacy and

[1] *In re* Access to Video Conferencing, Implementation of Sections 716 and 717 of the Communications Act of 1934, as Enacted by the Twenty-First Century Communications and Video Accessibility Act of 2010, Telecommunications Relay Services and Speech-to-Speech Services for Individuals with Hearing and Speech Disabilities, Petition of Sorenson Communications, LLC for a Limited Waiver of the Privacy Screen Rule, Report and Order, Notice of Proposed Rulemaking, and Order, CG Docket No.s 23-161, 10-213, 03-123, at ¶¶ 96-98 (Rel. June 12, 2023), *available at* https://docs.fcc.gov/public/attachments/FCC-23-50A1.pdf [hereinafter NPRM]. The Proposed Rule was published in the Federal Register at 88 FR 52,088 (Aug. 7, 2023), and is available at https://www.federalregister.gov/documents/2023/08/07/2023-16672/access-to-video-conferencing.

[2] Electronic Privacy Information Center, https://epic.org/ (2023).

cybersecurity issues.[3] EPIC routinely advocates before the Commission for rules that protect consumers from exploitative data practices,[4] including supporting protections for TRS users.[5]

II. The Commission should be explicit that providers cannot train AI using live data without meaningful consumer consent.

Training AI on individuals' personal data doesn't just amount to exploitation, it can also inflict serious privacy harms when the outputs of AI systems reproduce data from the training set. Here, a poorly managed AI could divulge the contents of people's video-conferenced conversations. As a result, the indiscriminate collection of data to feed AI risks chilling communication and participation in digital fora, is contrary to data minimization principles, and poses additional risks to vulnerable populations who need to be able to delete their personal information.[6] Misuse of communications data to train AI is occurring in prison settings.[7] There have already been documented instances of AI models being trained using purportedly private

[3] *See In re* Implementation of the Telecommunications Act of 1996: Petition for Rulemaking to Enhance Security and Authentication Standards For Access to Customer Proprietary Network Information, EPIC Petition, CC Docket No. 96-115 (Oct. 25, 2005), https://www.fcc.gov/ecfs/search/search-filings/filing/5513325075.

[4] *See, e.g.*, *In re* Empowering Consumers Through Broadband Transparency, Comments of CDT, EPIC, and Ranking Digital Rights, CG Docket No. 22-2 (Feb. 16, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/102161424008021; *In re* Location-Based Routing for Wireless 911 Calls, Comments of EPIC, PS Docket No. 18-64 (Feb. 16, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/10216148603009; *In re* Rates for Interstate Inmate Calling Services, Letter Comment of EPIC, WC Docket No. 12-375 (Dec. 15, 2022) https://www.fcc.gov/ecfs/search/search-filings/filing/121545964412.

[5] *See, e.g.*, *In re* Data Breach Reporting Requirements, Reply Comments of Electronic Privacy Information Center, Center for Democracy and Technology, Privacy Rights Clearinghouse, Public Knowledge, WC Docket No. 22-21, at 15-18 (March 24, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/1032465071814 [hereinafter EPIC et al Reply Comment].

[6] *See, e.g.*, EPIC, *Generating Harms: Generative AI's Impact & Paths Forward* 24-29 (May 2023), https://epic.org/wp-content/uploads/2023/05/EPIC-Generative-AI-White-Paper-May2023.pdf (section beginning with "Profits over privacy: increased opaque data collection").

[7] *See, e.g.*, 55 Civil Rights Groups Demand DOJ, NY Investigate AI Audio Surveillance in Prisons, Jails, Press Release, Surveillance Technology Oversight Project (Feb. 10, 2022), https://www.stopspying.org/latest-news/2022/2/10/55-civil-rights-groups-demand-doj-ny-investigate-ai-audio-surveillance-in-prisons-jails.

data.[8] The exfiltration of training data is also not a mere hypothetical.[9] Indeed, bans have already been implemented in both the private and public sector to prevent this kind of breach of data that has been "fed" into the model.[10]

In the TRS context, despite Commission rules requiring deletion of data at the end of a call, there are indications that providers are still retaining this information.[11] The Commission must ensure that TRS data is not used in this manner unless the TRS user has affirmatively and expressly consented to their personal information being used for this purpose following a clear and comprehensible disclosure of the risks associated with such use.

This misuse violates the confidentiality of communications and undermines cybersecurity best practices such as data minimization. Profiting from the content of communications by consumers who rely on TRS is simply inappropriate.

---

[8] *See, e.g.*, Benj Edwards, *Artist finds private medical record photo in popular AI training data set*, ArsTechnica (Sept. 21, 2022), https://arstechnica.com/information-technology/2022/09/artist-finds-private-medical-record-photos-in-popular-ai-training-data-set/.

[9] *See, e.g.*, Shotaro Ishihara, *Training Data Extraction from Pre-trained Language Models: a Survey*, ACL Anthology, Proceedings of the 3rd Workshop on Trustworthy Natural Language Processing (TrustNLP 2023) (July 2023), https://aclanthology.org/2023.trustnlp-1.23/.

[10] *See, e.g.*, Kate Park, *Samsung Bans Use of Generative AI Tools like ChatGPT After April Internal Data Leak*, TechCrunch (May 2, 2023), https://techcrunch.com/2023/05/02/samsung-bans-use-of-generative-ai-tools-like-chatgpt-after-april-internal-data-leak/; Dan Milmo and Agencies, Italy's Privacy Watchdog Bans ChatGPT Over Data Breach Concerns, Guardian (Apr. 1, 2023), https://www.theguardian.com/technology/2023/mar/31/italy-privacy-watchdog-bans-chatgpt-over-data-breach-concerns.

[11] *See in re* Data Breach Reporting Requirements, Comments of Accessibility Advocacy and Research Organizations, WC Docket No. 22-21, at 2 (Feb. 22, 2023), https://www.fcc.gov/ecfs/document/10223571503790/1 [hereinafter AARO Comment] ("recent analysis shows that some terms of TRS providers' user agreements conflict with or raise ambiguities about providers' compliance with TRS confidentiality requirements") (citing to Ex Parte of HLAA, TDI, et al., CG Docket Nos. 03-123, 13-24 ("TRS Privacy Ex Parte") (May 5, 2022), https://www.fcc.gov/ecfs/filing/10506819528704).

III. The Commission should clarify that its privacy protections extend to non-relayed content and to automated TRS tools that do not utilize a CA.

EPIC supports the Commission's proposals to expressly prohibit CAs from disclosing non-relayed content communicated in a video conference,[12] including TRS calls in which TRS is provided by automated process without a CA.[13] As advocates articulated in the docket on CPNI data breach reporting, the communications privacy of TRS users demands heightened attention to provider and third-party privacy and cybersecurity practices.[14] TRS users should have peace of mind that sensitive information such as their "medical history, disability status, financial situation, political views, relationship status and dynamics, and religious beliefs"[15] will not be inappropriately retained or disclosed merely because it was considered non-relayed content and therefore outside the scope of the rule. For example, a sidebar conversation between TRS participants about a doctor's appointment (or any subject matter) that is not intended to be relayed by the CA to the other TRS participants should be given at least the same level of protection as the communications the participants intended the CA to relay.[16] Similarly, the Commission should clarify that automated TRS tools without a CA are within the scope of the rule.

IV. Conclusion

We applaud the Commission's attention to the heightened privacy concerns experienced by TRS users and urge the Commission to be explicit about how TRS data should not be used to train AI without consent. We also urge the Commission to ensure it is fully protecting TRS

[12] NPRM at ¶ 96.
[13] *Id.*
[14] *See* AARO Comment at 2, 3, 6. EPIC supported these comments in its own Reply Comments. *See* EPIC et al Reply Comments.
[15] AARO Comment at 3.
[16] NPRM at ¶ 97.

users' sensitive information by clarifying that the rule applies to non-relayed content and automated tools. For any questions or additional information please reach out to EPIC Counsel Chris Frascella at frascella@epic.org.

Respectfully submitted, this the 6th day of September 2023, by:

Chris Frascella
Counsel
Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036

Jake Wiener
Counsel
Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036