PRAC3 (Privacy, Reputation, Accountability, Consent, Credit, Compensation): Voice Actors in AI Data-Economy

Tanusree Sharma[1], **Yihao Zhou**[1], **Visar Berisha**[2]
[1]Pennsylvania State University *
[2]Arizona State University
[1] tanusree.sharma@psu.edu

Abstract

Early large-scale audio datasets, such as LibriSpeech, were built with hundreds of individual contributors whose voices were instrumental in the development of speech technologies, including audiobooks and voice assistants. Yet, a decade later, these same contributions have exposed voice actors to a range of risks. While existing ethical frameworks emphasize Consent, Credit, and Compensation (C³), they do not adequately address the emergent risks involving vocal identities that are increasingly decoupled from context, authorship, and control. Drawing on qualitative interviews with 20 professional voice actors, this paper reveals how synthetic replication of voice without clear provenance or enforceable constraints exposes individuals to both reputational and security threats.

Beyond reputational harm, such as re-purposing voice data in erotic content, offensive political messaging, and meme culture, we document concerns about accountability breakdowns when their voice is leveraged to clone voices that are deployed in high-stakes scenarios such as financial fraud, misinformation campaigns, or impersonation scams. In such cases, actors face social and legal fallout without recourse, while very few of them have a legal representative or union protection. To make sense of these shifting dynamics, we introduce the PRAC³ framework - an expansion of C³ that foregrounds Privacy, Reputation, Accountability, Consent, Credit, and Compensation as interdependent pillars of data used in the synthetic voice economy. This framework captures how privacy risks are amplified through non-consensual training, how reputational harm arises from decontextualized deployment, and how accountability can be reimagined AI Data ecosystems. We argue that voice, as both a biometric identifier and creative labor, demands governance models that restore creator agency, ensure traceability, and establish enforceable boundaries for ethical reuse.

Introduction

Data sharing has long been a contested domain between individual contributors, professionals, and data controllers. Individuals or groups contribute data either deliberatively, whether in pursuit of social value, to receive financial compensation, or as part of their primary profession (Allen 1999; Lane et al. 2014; on Health Sciences Policy and on Strategies for Responsible Sharing of Clinical Trial Data 2015; Godard et al. 2003). These contributions are influenced by a variety of motivations, such as financial incentives from industry (Massiceti et al. 2021) and academia (Tseng et al. 2024; Sharma et al. 2023b), creative expression and social interaction on online platforms (Andalibi, Ozturk, and Forte 2017; Lee and Hong 2016), participation in public-interest initiatives like Mozilla Common Voice (Ardila et al. 2019), LibriSpeech (Panayotov et al. 2015) and AESDD (AESDD 2018). The European Commission estimates that data sharing has the potential to save billions of euros (EU 2015). Shared data are typically governed by various licensing frameworks, including Creative Commons (Lin et al. 2014; Russakovsky et al. 2015), Open Data Commons (ODC) (Miller, Styles, and Heath 2008), GNU General Public License (GPL) (License 1989).

Despite these practices, recent legal developments indicate increasing friction between AI companies and creative workers (Tenbarge 2024; Gero et al. 2025; Shan et al. 2023; Kyi et al. 2025). In 2024, a YouTube creator initiated a lawsuit against OpenAI, arguing the company transcribed millions of hours of video content to train models like ChatGPT without consent (Cho 2024). Likewise, voice actor Bev Standing filed legal action against TikTok regarding the unauthorized use of her voice in its text-to-speech feature (BBC 2021). Although companies like OpenAI reported that their training datasets consist of publicly available resources (OpenAI 2025), public access does not automatically grant legal or ethical approval for such usage (Gao et al. 2024; Hoffman 2015). Therefore, creative workers contend that their materials were gathered without authorization, credit, or financial remuneration, resulting in several lawsuits, purported violations of terms of service, and coordinated protests (Bloomberg 2024; Allyn 2023). These reflect broader concerns on unconsented use of their work for AI training, particularly when such work is copyrighted or personally attributable.

While prior work reasonably explored the risk of creative workers, particularly visual artists and writers, research on voice professionals remains limited. Much of the current discourse focuses on fairness in compensation, credit, and consent (Tenbarge 2024; Gero et al. 2025; Shan et al. 2023; Kyi et al. 2025; Gero et al. 2025) and frames Gen AI as a collaboration tool for creativity (Liu et al. 2024; Chakrabarty et al. 2024). In contrast, voice actors and narrators carry a unique

*Corresponding author: Tanusree Sharma

intersection of creative labor and biometric vulnerability. Unlike textual or visual data, voice is uniquely identifiable to a person (Aleksic and Katsaggelos 2006). Thus, voice contributors are prone to a wide range of harms, including unauthorized cloning, impersonation, reputational damage, and identity theft (Hutiri, Papakyriakopoulos, and Xiang 2024; Ekene Chuks-Okeke 2023); however these risks have received little systematic attention.

Moreover, voice actors and contributors played a foundational role in the development of speech technologies (Prahallad, Raghavendra, and Black 2010b,a; Tauberer 2010). A notable innovation was the early large-scale audio datasets, LibriSpeech, derived from thousands of contributions to LibriVox and other public domain audiobook platforms, underpinned early breakthroughs in automatic speech recognition and the voice assistants we use today (Van Horn 2007; Kearns 2014; Prahallad 2010; Panayotov et al. 2015). These contributions, originally made in the spirit of open knowledge and accessibility, have since been repurposed into commercial AI pipelines often without consent, attribution, or safeguards (BBC 2021). A decade later, these same contributions have exposed voice actors to a range of harms and may automate, devalue, or displace the very actors who created it. Yet, despite their centrality to the voice technology landscape, voice actors remain underrepresented in discussions of data labor and AI ethics and risk pertaining to the voiceprint (both a personal and professional tool for voice actors). To address this urgent gap, this study investigates how professional voice actors perceive, negotiate, and respond to risk in the generative AI landscape.

- **RQ1:** In what ways do voice actors recognize, interpret, and negotiate risk when engaging with digital platforms, clients, and publishers, given the rise of generative AI?
- **RQ2:** How do voice actors perceive the long-term risks associated with voice data?
- **RQ3:** How do voice actors' perceptions and lived experiences of risks contribute to forming threat models in assessing risk over time?

To answer these questions, we interviewed a total of 20 voice actors at different stages of their careers and in different work modes (e.g., freelancers, contract workers, and studio owners). We found that voice actors face unique challenges that are different from other creative workers, including: **1) Biometric Identity Risks**: Voice data combines creative work with biometric identity, thus exposing voice actors to unique risks of unauthorized cloning, identity theft, and reputational harm when their recordings are misused in unauthorized illegal contexts. **2) Long-Tailed Risks:** Voice actors face ongoing and evolving risks as their recordings can be continually reused, repurposed, redistributed, and integrated into new AI models long after initial consent, often without their knowledge or further compensation. **3) Difficulties in Data Traceability and Control:** Voice actors experience a significant loss of control over their voice data post-delivery, with an absence of effective mechanisms to track how their voice files are used, shared, or altered, particularly for AI training or cloning. Based on this context-dependent risk, we propose **PRAC³** framework, which expands the existing C³ (Consent, Credit, Compensation) to adapt emerging risks related to voice in Privacy, Reputation, and Accountability.

Related Work

Voice Actors' Risk Beyond the Three Cs

Voice actors have become focal points of concern with the rise of AI-generated speech. Unlike text or image data, voice data is biometric, uniquely identifying and intimately tied to an individual. Recent works started to catalog ethical and safety risks posed by synthetic voice cloning from impersonation scams contributing to swatting attacks and financial fraud and in malicious deepfakes that fuel misinformation (Hutiri, Papakyriakopoulos, and Xiang 2024). Critically, these risks often arise from multi-facedted interactions among stakeholders e.g. a company releasing a model (Kastrenakes 2021), a malicious actor using it, and victims (Hutiri, Papakyriakopoulos, and Xiang 2024) and voice owners suffering the consequences, making it hard to assign accountability (Agnew et al. 2024). Voice actors face challenges at this intersection of creative labor and biometric vulnerability because their voices are not only artistic output but also their personal identifiers with overlapping risks. Moreover, voice actors are discovering unauthorized voice clones of themselves being distributed online, such as, clone voices of voice actors with foul and offensive language, causing her irreparable harm (Kastrenakes 2021) and even celebrities have voiced concerns where Scarlett Johansson's AI-generated voice without consent (Tenbarge 2024).

Recently, IAPP advocates stronger protections than those afforded by existing frameworks (3 C's) for visual or textual creators (Ekene Chuks-Okeke 2023). Notably, when current law often falls short where in the U.S., a person's voice itself is generally not protected by copyright (only specific recordings are) (Ekene Chuks-Okeke 2023). For example, simply giving credit to an original artist when an AI mimics their style does not prevent economic displacement or the emotional impact of seeing one's style copied by a machine (Kyi et al. 2025). Likewise, one-time compensation (such as paying for a data license) might not be adequate if the AI model continues to derive value from an artist's work indefinitely a concern related to the long-tailed nature of generative AI benefits (Nagano 2025). Thus, voice actors are part of a broader creative workforce that encounters multifaceted risks in various forms. A primary client may repurpose voice data beyond the scope of the original agreement, such as for future AI training or product expansion; AI companies often train models on massive repositories of "publicly available" data such as audiobooks or demo reels; secondary creators may use voice samples as background content, remix them into memes, or manipulate them with AI tools for entertainment without authorization (Kastrenakes 2021); adversarial actors have used cloned voices to perpetrate fraud, financial scams (Bateman 2020; Jasserand 2024).

In our work, we investigate how voice actors face evolving risks beyond consent, credit, and compensation, proposing a dynamic threat model to assess long-tailed risks resulting from repurposing in the generative AI era.

Privacy Risks in Data Sharing

Today's consumer-facing systems, such as recommender systems, search engines, and more recently, large language models, often provide personalized services by processing vast amounts of data. There are two different ways data owner shares their data: deliberately and in an implicit manner. Implicit data sharing happens when users naively consent to terms of service, as is common with applications like ChatGPT (Yu et al. 2024), search engines (Sharma et al. 2024), and social media (Kaushik et al. 2024; Sharma et al. 2023a) platforms, web-crawled public user data (Schuhmann et al. 2022; Baroni et al. 2009; Thomee et al. 2016; Baumgartner et al. 2020). In contrast, deliberate data sharing occurs when individuals knowingly contribute to public datasets (Sharma et al. 2023b; Ardila et al. 2019; Kearns 2014), often presenting tangible benefits like monetary rewards, research contributions, or social support or as a part of their primary profession (Allen 1999; Lane et al. 2014; on Health Sciences Policy and on Strategies for Responsible Sharing of Clinical Trial Data 2015; Godard et al. 2003). This includes ML data workers and creative contributors but also participants in open voice data initiatives like Mozilla Common Voice and LibriVox, whose recordings have been foundational to speech technologies (Panayotov et al. 2015; Tauberer 2010).

A major challenge for data contributors is the lack of mechanisms to manage privacy, ownership, and value over time (Sharma et al. 2024; Sambasivan et al. 2018). In the case of deliberate data sharing, especially for voice, privacy risks are increasingly entangled with issues of long-term control and commodification (Panayotov et al. 2015). As generative AI models evolve and are reused across multiple applications, original contributors often lose visibility into how their data is being leveraged by whom, and to what end. This shift has led data owners to reframe privacy not only as a matter of control, but also as a function of data valuation and fair compensation(Romanosky and Acquisti 2009; Acquisti, John, and Loewenstein 2013).

Despite the length of research in data sharing and governance, to date, *there are no solutions that help data owner assess their risk during data-sharing activities*. Existing frameworks such as, such as NIST (Lefkovitz and Boeckl 2020), ISO/IEC (Purdy 2010), CSA CCM (CCM 2024), and GDPR (GDPR 2024), though designed for risk assessments of federal information systems and organizations, have not been adapted to provide data owners with tools in understanding risks and the value of their data over time.

Method

We conducted an interview study with 20 voice actors to better understand how generative AI risks, particularly synthetic voice replication, impact voice actors in terms of reputational, privacy and security threats. The study was approved by our university's Institutional Review Board (IRB).

Participants Participants were recruited via email, with an explanation of the research and an invitation to participate in an interview. Our sample consisted of freelancers, contract workers, and full-time professionals, with voice acting experience ranging from 4 to 20 years. Each participant was assigned a random number (e.g., P01) for anonymity.

Interview Process We developed a semi-structured interview protocol that asked participants about their typical workflow and data sharing practices, including how they select platforms for voice work, auditioning processes, contract experiences, and tools used; their experience and awareness of generative AI and the risks related to synthetic voice replication; their opinions on data ownership and consent; and the privacy risks related to their work, such as synthetic voice misuse in unauthorized contexts.

Where participants raised topics related to our research goal but not covered in our interview protocol, we asked follow-up questions; for example, P4 mentioned experience watermarking voice data, so we asked more about current watermarking practices. Interviews lasted between 40 and 70 minutes and averaged approximately 60 minutes. All interviews were conducted in English.

Data Analysis Interviews were recorded and transcribed over Zoom and manually corrected as necessary by the first and second authors. To answer the research questions, we adopted a deductive-inductive approach to coding the interview transcripts. We employed the following deductive codes: Participant Category, Awareness and Understanding of AI Risks, Workflow and Practices, Ownership and Compensation, and Privacy and Security Concerns.

Each interview transcript was coded in several rounds. The authors first coded seven transcripts and created an initial codebook that included inductively generated themes. After that, the authors reviewed and revised the codebook. For example, the Participant Category code did not exist in the codebook at the beginning, but after the first round of coding, we found that the participants' experience as voice actors and the resources available to them when encountering legal and data ownership issues varied significantly. As a result, we added the Participant Category code to better capture the diversity of experiences and resources across participants. The authors then coded two additional transcripts at a time until all transcripts had been coded. Finally, the authors followed a thematic analysis process (Clarke and Braun 2017) to generate themes that answered research questions and created four different user personas, using a shared document to precisely define the themes.

Results

Personas of Voice Actors

From our list of 20 participants, we created four personas based on years of experience and availability of resources, as shown in Table 1. The four significant personas are: (a) Solo Defender (High experience, Low resources); (b)Emerging Professional (Low experience, Low resources) ; (c) Well-Equipped Expert (High experience, High resources); and (d) Supported Newcomer (Low experience, High resources). For instance, common traits of Supported Newcomer personas include having less than 10 years of experience, strong home studio setups, reliance on direct client relationships with occasional platform works, being proactive in using AI riders from NAVA, and often opting out if client disagree.

Persona	Experience	Resources	Pain Points
Solo Defender	High	Low	Resource-constrained; hard to identify risky clients or detect covert data scraping; limited control over data usage.
Emerging Professional	Low	Low	Hard to recognize vague clauses and terms; Worry about AI misuse; limited AI/data literacy and legal/contract knowledge.
Well-Equipped Expert	High	High	Brand-conscious; proactively negotiates AI-related clauses and pricing; sensitive to reputation harm caused by data misuse.
Supported Newcomer	Low	High	Supported by agents or platforms on vetting and contracting; limited understanding of AI risks; rely on third-party safeguards.

Table 1: Personas of Voice Actors

They often have their own representative to assess contracts and negotiate client compliance with AI clauses. This group holds deep concerns over AI risks, especially unauthorized cloning and unauthorized voice usage for AI training. P12 (a Supported Newcomer persona) shared their experience explaining how their agent assessed a project:

> *"You're handed a contract, and you glance at it, and you know you got to sign it there ... I didn't go over it with a fine tooth comb. In one of TV affiliates projects, my agent asked, we need to confirm that you're not going to use this for AI. They said we're not going to confirm anything. And my agent and I were both-we're not going to do this".*

Whereas the Solo Defender persona involves voice actors raging from mid-level experience to senior freelancers. They have reasonable knowledge of technology and media IP. They handle their own contracts and have systemic awareness of AI risks across sectors. They share common pain points and concerns, such as covert data scraping from public platforms and lack of enforceable standards for dataset auditing, as P5 explained,

> *"I did get an offer, and I try to research it as much as possible. And I do ask, you know, what is this going to be used for... before I engage in even auditioning."*

Indication of Risk Through Interaction

In their routine professional activities, voice actors work across a range of sectors such as, commercials & advertising, followed by audiobooks, animation & cartoons, and E-Learning & educational content, video games, and podcasting & audio dramas, dubbing & localization, live performance & theatrical productions, each showing high demand across the industry. We found a reservation of voice actors to work on Text-to-Speech (TTS) & AI Voice Training project due to both normative and practical concerns. For all participants, voice acting was their primary profession, typically following a structured workflow: (a) discovery of the work; (b) Audition ; (c) Contracting; (d) Recording and File sharing. In this section, we lay out the risks in each stage of their interaction, in particular risks pertaining to with advanced AI landscape, as shown in Figure 1.

Discovery. The first phase involves voice actors seeking projects aligned with their skills, interests, and availability. Participants identified three primary channels for finding work: commercial platforms (e.g., Voice123, Amazon ACX), social media job postings (e.g., Facebook, Twitter, LinkedIn, Bluesky, Discord), and agent representation.

In this phase, participants explained a key concern, which was the difficulty in distinguishing legitimate opportunities, particularly when platforms allow anonymous clients. Thus, determining if the project is legit or a means to collect voice data for unconsented use in Text-to-Speech (TTS) applications, often challenging for voice actors. Participants expressed a preference for working with agents or clients who engage in direct, identifiable communication, allowing for dialogue and verification in contrast. However, a very small number of participants had access and the means for agents or direct connections with publishing houses and individual clients, which largely contingent on the actor's experience and the professional network they had developed over time. This highlights a level of gatekeeping and structural advantage not available to less experienced voice actors, leading to risks of their voiceprint ending with bad actors.

Audition. Auditions serve as a gateway for voice actors to secure roles, yet this crucial stage remains largely unregulated in terms of how submitted samples may be used beyond the selection process. Participants mentioned producers or client often shielded by non-disclosure agreements (NDAs) signed by voice actors, where the actors themselves typically operate without reciprocal legal protection. The current industry norm relies on informal trust. We encountered incident where audition sample were indeed used, but later remediate by booking the artist, as P11 recounted,

> *"It's just an unspoken agreement, you have to sort of trust... I've only had once-client used my audition for the job. But they booked me later, so it was fine."*

Participants consistently identified this auditioning phase as one of the most vulnerable to misuse particularly regarding unauthorized AI training or voice cloning. To mitigate these risks, voice actors rely on informal, ad-hoc strategies, such as, mark as read flag if (a) requests for unusually long audition samples (b) lack of communication from intermediaries (e.g, agent, client, casting director). As P18 said

> *"Usually when you do a read like that, it's between a minute to 5 minutes long based on the project types like, commercial might need longer one where au-*

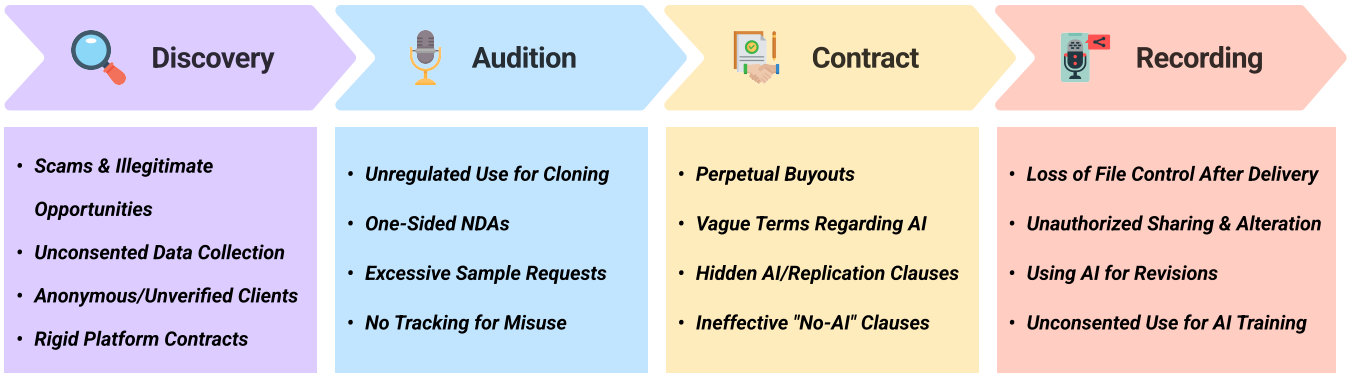

Figure 1: Risks and AI-related threats in different stages of voice acting work, including discovery, audition, contracting, recording and file sharing.

> *diobook should not need more than 60s. If its longer, there is something off with the client."*

Some participants mentioned technical deterrents, such as inserting beeps into their samples to prevent unauthorized use. However, most rejected this approach due to concerns that it compromised the quality and may jeopardize job opportunities. Notably, several participants suspected that their auditions had indeed been misused, yet felt powerless due to no means of tracking or legal recourse.

Contract Negotiation. In contract negotiations, voice work involves credit, consent, and compensation. Participants reported credit practices, such as, audiobook clients often provide public-facing credit to narrators, but rare in commercial or corporate contexts. They mentioned varied compensation including, session-based fees, time-limited buyouts, and perpetual rights. In the era of generative AI, compensation terms like *"in perpetuity buyout"* are seen as red flags, often signaling potential for AI repurposing if pay is not high. P12, the original male voice of a voice assistant tool of major tech, recounted how a one-time session and a yearly non-compete fee evolved into widespread, unauthorized use of his voice.

> *" It was released 5 or 6 years back. I regret not having a lawyer review the contract, which included broad terms like 'in any form or technology now known or unknown, in perpetuity.' I later found out my voice is rented to Y and Z companies. Interestingly got to know that from my daughter and friend. That didn't feel good. I hadn't understood how my voice would be used, but for a while, people kept asking if I did a hotel ad in Berlin or other projects. My voice ended up in explainer videos, commercials, and even a video game chatbox without additional pay. Since then, I've renegotiated for higher compensation. Still, the original deal locked me into a much lower rate especially compared to the female voice, who reportedly earns around $250k a year."*

This highlights mismatch between contractual terms and long-term value in the AI era. Participants are becoming more vigilant about ownership risks. As P3 noted, actors often refer to *"voice ownership"* without fully understanding its implications. *"We have signed away the right to the performance and not the voice print."*

To address concerns with three Cs, participants cited the NAVA community-developed AI rider, which is becoming a standard to attach during contracts. Several participants shared troubling experiences. P1 described a case where their voice with client for a video game was later synthesized with AI despite a *"No-AI"* clause the developers never saw. P4 also recalled a contract in which a clause allowing voice replication was buried in Exhibit A, unseen by the actors. Such cases highlight how vague or inaccessible legal language leaves voice actors, especially newcomers vulnerable to exploitation. *"Exhibit A wasn't even seen by the actor. The publisher signs it"*

Recording & File Sharing. In this phase, a common set up of voice actors is - recording in home studios using XLR mics, audio interfaces, and DAWs like Reaper or Audacity. They typically record in three model (a) home studio, (b) remote sessions via Source Connect, or (c) on-site studio sessions. They share files through platforms like WeTransfer (valued for simplicity and notifications), Dropbox, Google Drive (for large or ongoing work), or email (for small .mp3 auditions). They mentioned platforms like Voices.com or ACX sometimes handle the upload internally. This stage carries significant risks, primarily loss of control and transparency. Once files are sent, actors have little visibility into how they are used, shared, or altered. As P14 noted:

> *"There's no way to verify that a client sticks to their usage agreement... unless I catch it in the wild. Once it's downloaded... they might share with someone else, chop it up, and send it off. I don't think none are using such technologies in industry now. Maybe there could be something in that initial audio file... so that if an AI clone is made, it's detectable."*

Participants also raised concerns about "pick-ups"—where clients use AI to mimic voices for minor revisions rather than hiring the actor again. Many expressed frustration that no watermarking or traceability measures are in place to detect such misuse. Further platform-specific concerns emerged, for example, P8 highlighted potential conflicts of interest with Amazon ACX, questioning whether sub-

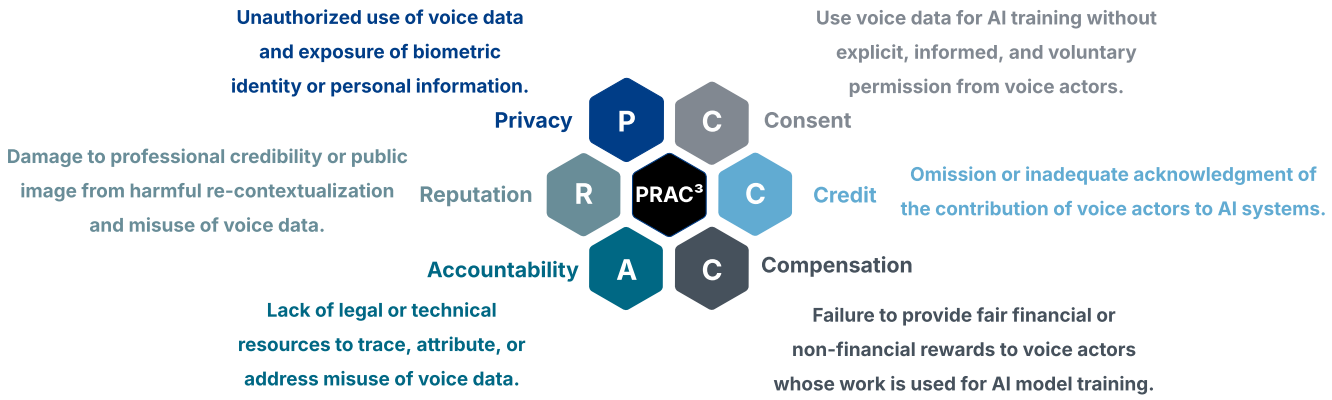

Figure 2: The PRAC³ framework, including six risk dimensions in the use of voice actors' data in the context of generative AI: Privacy, Reputation, Accountability, Consent, Compensation, and Credit.

mitted voice data could be repurposed for amazon's product. Across the board, actors emphasized the lack of post-delivery tracking and growing fear of their recordings being used for AI training.

Current & Long Term Risks Perception

Our analysis with professional voice actors revealed awareness of both current vulnerabilities and future threats, beyond the three Cs, particularly around privacy, reputation, and accountability.

Security and Identity Concerns Participants expressed growing concern over the biometric nature of voice data and the ease with which it can now be cloned and reused without authorization. Several actors identified the potential for fraud and impersonation particularly, in financial or emergency contexts. For instance, P16 noted

> *"Scammers can now... call you and say 'Mommy, I'm being hurt' using your kid's voice. And you don't know if it's real. Its really frightening. My voice is out there more than an average users."*

Some reported concerns on voice authentication in banking. Meanwhile, actors like P16 pointed to the existential challenge of deepfakes, describing it as *"Not being able to verify your own voice because someone has stolen it.. next-level voice theft."*. P8 explained -

> *"If financial institutions use voices... that's not a good idea considering how easy it is to duplicate. I also sometime wonder- banks that ask for voice verification... Is it being used to train something else?"*

One participant with a cybersecurity background (P6) emphasized that some deepfake uses cross into serious crime, noting incidents where AI-cloned voices were used for *"swatting"* (calling in fake threats) and other dangerous hoaxes. These concerns underscore the shift from theoretical risk to practical harm, particularly for security and safety of voice actors in their personal life.

Reputational and Ethical Risks Voice actors also raised serious concerns about their voices being used in ways that contradict their values and can often damage their personal standing. We found scenarios where some participants found their voice being mismassed to create AI-generated voice content in controversial media such as, political, controversial media. One actor recalled a case where P4 mentioned-

> *" I initially worked on a anime character which was normal. then they made that character do AI-generated porn... that reflects badly on me, which was never consented."*

Some also feared their voices could be embedded in propaganda or defamatory content, with no clear mechanism for recourse or correction. P17 described an unsettling experience of hearing accidentally a TV commercial on political agenda in gender issues which sounded like her own voice which she never recorded. This lack of control over one's digital likeness raises questions about the professional and personal boundaries in the age of generative AI.

Accountability and Legal Uncertainty. Participants expressed frustration over the lack of enforceable rights and mechanisms to trace, remove, or contest the misuse of their voice. For example, P117 described a situation in which a TikTok user initially perceived as a fan used a voice sample from her website to create a reel video:

> *"At first, I hear my voice in the background, it seemed benign. Then I realized there was AI to clone certain words I never said. If those memes become more extreme, who is accountable– me, the person who cloned, or the TikToker?'*

Beyond the concerns of accountability, some participants added concern of professional and economical reputation. P17 highlighted how their voice association with low-quality productions or cloned by individuals could damage his credibility, as audiences might conflate the synthetic performance with the original artist. Similarly, P3 explained

> *"I don't doubt one day some content's gonna feature my voice . . . and I'm very much scared for that day to navigate legal world... more scared when legitimate companies and criminals alike, now a temptation to "rip off everybody" by harvesting voices, and our legal system is only starting to grapple with it."*

ID	Scenario	Incident (Participant)	Analysis using PRAC³ Framework
1	Audition sample reused in national commercial	P17 discovered her voice in an ad she never recorded (P17)	**PRAC³ Domain:** Consent, Compensation, Accountability **Threat Agent:** Client/Studio **Asset at Risk:** Voice data, creative labor **Potential Impact:** Unauthorized commercial use; loss of income; reputational risk **Mitigation Status:** None – discovered post-facto
2	Voice used in AI-generated adult content	Game mod used AI to create pornographic scenes with actor's voice (P7)	**PRAC³ Domain:** Reputation, Consent, Accountability **Threat Agent:** Third-party modders **Asset at Risk:** Public persona, moral integrity **Potential Impact:** Defamation; emotional distress **Mitigation Status:** Unreported; no recourse
3	Exhibit A clause allows post-production cloning	Audiobook contract allowed voice replication without notice (P4)	**PRAC³ Domain:** Consent, Compensation, Accountability **Threat Agent:** Publisher **Asset at Risk:** Voice likeness; residual earnings **Potential Impact:** Job displacement; IP erosion **Mitigation Status:** Discovered post-signing
4	AI voice scam using child's cloned voice	Scam calls using cloned voice of loved one (P16)	**PRAC³ Domain:** Privacy, Identity, Accountability **Threat Agent:** Cybercriminals **Asset at Risk:** Biometric identity **Potential Impact:** Financial fraud; emotional harm **Mitigation Status:** Hypothetical/precautionary
5	Podcast platform AI-translates and clones voice	Large tech [Y] translated podcaster's voice without opt-out (P19)	**PRAC³ Domain:** Consent, Privacy, Accountability **Threat Agent:** Platform provider **Asset at Risk:** Voice data; linguistic identity **Potential Impact:** Unconsented speech generation **Mitigation Status:** Actor manually obstructed usage
6	No disclosure of voice reuse for AI training	P4 reported clause only found post-distribution	**PRAC³ Domain:** Consent, Privacy, Compensation **Threat Agent:** Client **Asset at Risk:** Voice training data **Potential Impact:** Unpaid AI training use **Mitigation Status:** No consent captured
7	AI-generated voice used in foreign language translation	Large tech [Y] used AI to translate podcaster's voice without clear opt-in (P16)	**PRAC³ Domain:** Privacy, Consent, Accountability **Threat Agent:** Platform **Asset at Risk:** Voice identity; language authenticity **Potential Impact:** Loss of control over voice use, misrepresentation **Mitigation Status:** Voice actor manually obstructed feature with background audio
8	Audition samples used without hiring actor	Actors heard their audition voices in released work (P14, P16, P17, P18, P20)	**PRAC³ Domain:** Consent, Compensation, Credit **Threat Agent:** Client/Producer **Asset at Risk:** Audition recordings; performance data **Potential Impact:** Unpaid labor; reputational confusion **Mitigation Status:** Typically undiscovered until after release
9	Voice used in modded game porn content	AI-generated adult content using voice actors' characters (P7)	**PRAC³ Domain:** Reputation, Privacy, Accountability **Threat Agent:** Third-party users **Asset at Risk:** Character alignment; public image **Potential Impact:** Moral distress; brand damage **Mitigation Status:** No action taken; actors unaware until fans reported

Table 2: Examples of reported data-misuse and AI-related incidents affecting professional voice actors (Cases 1–9).

ID	Scenario	Incident (Participant)	Analysis using PRAC³ Framework
10	Hidden AI training clauses in audiobook contracts	Exhibit A allowed voice replication post-recording (P4)	**PRAC³ Domain:** Consent, Accountability, Compensation **Threat Agent:** Publisher **Asset at Risk:** Creative control; residuals **Potential Impact:** Job replacement by AI; under-compensation **Mitigation Status:** Clause discovered only post-facto
11	Client reuses voice clip across projects without permission	P17's voice reused in ad without consent	**PRAC³ Domain:** Consent, Accountability, Credit **Threat Agent:** Client **Asset at Risk:** Vocal performance; authorship **Potential Impact:** Unauthorized branding; reputational risk **Mitigation Status:** No prior notification; discovered incidentally
12	Scam calls using AI voice cloning of relatives	Actors fear scammers using their voice for fraud (P3, P16)	**PRAC³ Domain:** Privacy, Identity, Accountability **Threat Agent:** Cybercriminals **Asset at Risk:** Biometric voice identity **Potential Impact:** Financial scams; family trauma **Mitigation Status:** No technical prevention mechanisms
13	AI contracts lack explicit voice usage limitations	Contracts omit AI voice use clauses (P14, P1)	**PRAC³ Domain:** Consent, Privacy, Accountability **Threat Agent:** Clients/Platforms **Asset at Risk:** Legal rights over voice data **Potential Impact:** Non-consensual reuse or AI training **Mitigation Status:** Actors often overlook contract language
14	Perpetual license buried in email agreements	Clients assume full rights from email threads (P10, P18)	**PRAC³ Domain:** Consent, Compensation, Credit **Threat Agent:** Clients **Asset at Risk:** Work ownership; royalties **Potential Impact:** Lack of residuals; misappropriation **Mitigation Status:** No formal legal review of communication
15	Replacement by AI for minor roles or demo work	Lost work for minor roles to AI-generated voices (P14)	**PRAC³ Domain:** Compensation, Reputation, Accountability **Threat Agent:** Clients **Asset at Risk:** Job opportunities; creative career pathways **Potential Impact:** Job displacement **Mitigation Status:** Community advocacy; union action (no technical protection)
16	Voice licensed and mass redistributed via third-party	Large tech company licensed actor's voice to third-party platforms (P12)	**PRAC³ Domain:** Consent, Compensation, Accountability, Privacy **Threat Agent:** Clients **Asset at Risk:** Voice data; public image **Potential Impact:** Ongoing uncompensated use; loss of control; reputational risk **Mitigation Status:** Attempted renegotiation failed

Table 3: Examples of reported data-misuse and AI-related incidents affecting professional voice actors (Cases 10–16).

These difficulties were particularly severe for non-union actors, who frequently did not have the financial or institutional backing necessary to explore abuses or seek redress. With many intermediaries, such as, casting agents, platforms, production studios for a project, standing between them, identifying source of harms, and tracing accountability becomes a near-impossible task.

Conceptualized Framework of Threat Model to Assess Risks

As the voice industry intersects increasingly with generative AI, voice actors face distinct and compound risks to their identity, labor, and safety. These risks are structural, embedded in how digital labor is extracted, synthesized, and monetized.

Based on the earlier sections on risk indicators through different phases of voice actors interaction to digital platforms as well as their experienced and perceived risks, we proposed a PRAC³ framework. This offer a conceptual tool for threat modeling these long-tailed risks, especially in assessing harms that emerge over time and beyond contractual boundaries. PRAC³ stands for ***"Privacy, Reputation, Accountability, Consent, Credit, Compensation"***. Each dimension represents a critical vector of exposure or harm for voice actors in the AI data economy. **Consent, Credit, Compensation** presents foundational rights which often

overlooked or bypassed in AI data pipelines. newly added components from voice actor's experience: **Privacy** which presents breaches of biometric identity through cloning or surveillance; **Reputation**, which represents harm from voice misuse in misaligned, offensive, or deceptive contexts and finally; **Accountability** which present legal and technical gaps in traceability and recourse when voice actors data is misused by adversarial actors and harm general users.

Voice actors experience **three archetypal threat scenarios** that encapsulate both direct and downstream risks. These scenarios highlight how harm is not limited to the moment of data creation but often arises through redistribution, secondary use, and platform-driven commodification.

(a)Voluntary, non-monetary contributors: Actors donate voice data for public good, only to have it later surface in unauthorized commercial tools.

(b) Monetized contractual contributors: Initial legal agreements include ambiguous language often enabling resale, transfer, or indefinite reuse of voice data, especially following corporate changes.

(c) Secondary, informal misuse: Legally recorded voices leak into meme culture, satire, or political propaganda via AI tools, distorting public perception and damaging actors' professional standing.

Across all scenarios, key assets are voice recordings with identifiable voice features, voiceprint which is a unique vocal fingerprint capable of identification or cloning, reputational credibility, and contractual protections. When a voice actor performs, they manipulate multiple acoustic and articulatory signals to create different characters, emotions, or identities. These changes affect the perceived voice, but the underlying biometric voice signature often remains partially detectable by machines (e.g., AI voice recognition); even if data is anonymized before being shared, advanced analytics or cross-referencing with other datasets could re-identify contributors.

Table 2 and 3 illustrates PRAC³ framework by mapping real-world incidents shared by voice actors to the six dimensions. Each case illustrates how risks unfold across time and contexts: P7's incident where a modder used AI to generate explicit content using a recognizable voice from a game voice character a violation of Reputation, Consent, and Privacy.

Discussion

Ethical Frameworks: From C³ to PRAC³

Our work broadens the discussion of ethical AI data use by expanding the *"C³"*(Consent, Credit, Compensation) to PRAC³, adding Privacy, Reputation, and Accountability, which emerged through our findings and are important dimensions for long-term risk assessment. Prior work centered on creators' consent to their data and receive attribution and payment (Kyi et al. 2025; Blaising and Dabbish 2022). PRAC³ model can capture context-transcending risks posed by generative AI, for instance, how voice actors' *"vocal identities"* can become decoupled from context, authorship, and control in AI systems. Our findings reveal that voice, as a unique identifier, can be misused by clients or downstream users, causing harm to contributors' personal and professional identities. PRAC³ thus reframes voice actors as stakeholders, not just content sources, to offer a comprehensive model for assessing risks.

Privacy, as a pillar, encourage rethinking voice data not merely as creative output but as biometric personal data. Voiceprints which is central to voice actors' identity, are often scraped or shared without consent, echoing Zuboff's "surveillance capitalism," where human experience becomes unconsented raw material (Zuboff 2023). Our findings present that voice actors' sign a contract for their voice performance, not the voiceprint. Despite growing legal recognition (e.g., Illinois' BIPA (Cook 2024), EU AI Act (Act 2023), CCPA (Kagan 2020)), our findings reveal widespread misuse, particularly in privacy, security, and safety, due to a lack of provenance. Once voice data is embedded in models and spread across platforms, it's nearly impossible to trace or retract. Unlike image watermarking, to the best of our knowledge, robust voice provenance tools remain undeveloped (Pantiukhov et al. 2024; Kang et al. 2022). Legal protections lag, with gaps illustrated by the TikTok text-to-speech case, where a voice actor's work was repurposed without her knowledge (Kastrenakes 2021). Further, we found voice data reused in controversial memes, raising unresolved questions of accountability regarding whether to attribute the harm to secondary content creators who used the voice sample or the original voice actors whose voice been used. This indicated reciprocal reputational harm for voice actors. By positioning voice data as personal data tied to privacy, reputation, and accountability, our work advances frameworks for voice data governance in AI.

Long-Tailed Risks and Novel Threat Modeling

A key contribution of this paper is its threat modeling of long-tailed risks that emerge over time and across institutional boundaries, beyond immediate consent violations (Code and Culture 2024), by highlighting the need for anticipatory risk assessment, mainly explored in high-stakes security areas (A3MLAnticipatory 2025; Zarochintcev 2021). PRAC³ framework advances this by integrating baseline risks (C³: Consent, Credit, Compensation) with evolving and future threats with a context-dependent manner (Nissenbaum 2004) where each risk scenario defines assets (e.g., voiceprints), identifies threat actors, system or human vulnerabilities, and potential consequences for voice actors such as identity misuse, reputational damage, and clarify assumption and boundary for threat models. Our qualitative data illustrates these risks, where a voice actor's character was used in AI-generated pornography; others found their voices endorsing political messages or were rented internationally without consent. Such decontextualized deployments lifted voices from their original intent and violate personal and professional credibility. PRAC³ addresses these temporal and cross-context risks of how privacy is compromised through non consensual AI training, reputation is damaged by misaligned use, and perpetuates fraud and scam.

In effect, PRAC³ functions as a forward-looking frame-

work to encourage data ethics beyond bias and fairness audits, toward systemic. For instance, PRAC³ can situate alongside established frameworks such as NIST's risk assessment process and ISO/IEC information security principles to introduce explicit threat modeling elements for voice for voice actors and people whose voice data are more exposed than others, such as journalists, political personnel, TV personalities, podcasters, etc, particularly in the privacy and reputation category. . We believe this framework will provide means for researchers and practitioners to anticipate low probability but high impact events and institutional failure points (such as when voice data travels through many hands and jurisdictions), rather than leaving voice actors to fight case-by-case battles.

Digital Labor, Exploitation and Precarity

Credit and Compensation in PRAC³ affirms that voice data constitutes creative labor, situating voice acting within broader critiques of digital labor and platform exploitation. Our interviews reveal systemic issues familiar in gig economies, such as, power asymmetries, opaque contracts, and precarious work (Zhang et al. 2022; Liang et al. 2024). Many voice actors sign away rights *in perpetuity* for a one-time fee, often without understanding long-term implications with a lack of union protection. Unlike typical gig workers, voice actors go through auditions, yet legal safeguards are often absent in this stage. While AI systems can now learn from minimal samples, our study suggested this phase can lead to risk in displacing entry-level jobs, such as audiobook narration, with low-emotion synthetic alternatives and potentially eroding future labor opportunities, especially for newcomers.

Our findings show voice actors frequently unaware of how their recordings would be reused. Some voluntarily contributed to early datasets (e.g., LibriSpeech (Kearns 2014)), which were later pivotal in training generative AI. Yet, a decade later, these same contributions have exposed voice actors to a range of risks. In effect, voice actors' labor is being commodified and endlessly monetized by others, a pattern of algorithmic exploitation comparable to how other AI training data (art, code, writing) have been harvested without rewarding the original creators. Another reflection from our study, *"I wish I had a lawyer 5 years back"*, referencing how their voice was later "rented out" in global ads and games, without compensation. This underscores a critical mismatch between initial contract terms and the enduring value of data in AI systems. This exemplifies a mismatch between contractual terms and long-term value in the AI era. As Gray and Suri (2019) and others have noted, AI systems are fueled by millions of underpaid workers performing repetitive tasks under precarious conditions (Gray and Suri 2019; Sharma et al. 2025; Sharma 2024).

PRAC³ expands the ethical lens by connecting credit and compensation with reputation and labor precarity. Voice actors fear that low-quality synthetic or cheaply made AI clone reproductions of their voice can erode the actor's credibility, adding a new layer of workplace harm, reputation damage, and market displacement, atop the more traditional concerns of missing credit or payment. Currently, SAG-AFTRA and IATSE have pushed for contractual protections ensuring consent, credit, and compensation for performers' contributions to AI systems (Communications 2024). PRAC³ framework provides a conceptual backbone for these demands, factoring in three new component reputation, accountability, and privacy.

Conclusion

We shed lights on an overlooked area of creative work related to voice which is the current and upcoming commodities in Generative AI model advancement. By interviewing voice actors, we uncover risks of how voice data functions as both a creative product and a biometric marker, placing this community for prolonged challenges that go beyond conventional consent, credit, and compensation. We introduce PRAC³ framework to expand the ethical landscape to include Privacy, Reputation, and Accountability to offer a holistic model for assessing and mitigating these risks. As AI technologies continue to evolve and commodify human expression, this work underscores the urgent need for governance models, legal protections, and technical solutions that center the rights, identities, and labor of voice actors. Tackling these issues is crucial not only for their personal and professional dignity but also for establishing a just and reliable synthetic media landscape.

Ethics Statement

The PRAC³ framework proposed in this paper is derived mainly from the information provided to us by the respondents in the interviews. We did not focus on any data specific to individuals or vulnerable groups. Therefore, we do not foresee that the proposal and development of PRAC³ will cause ethical harm.

However, we do note some potential ethical issues. The coverage of our interview subjects is not comprehensive in the context of geography. Although further research is still in progress, at present, our interviewees are all from the United States. Although our summary of voice actor workflows, classification methods, and interview guidelines does not focus on regionally specific practices, and we try to make the process compatible with a more diverse AI governance environment, we cannot completely avoid this bias.

In addition, because our conclusions are mainly derived from interview data, we may have overlooked some undisclosed practices. Therefore, we emphasize that PRAC³ is a conceptual framework and may limit the comprehensive understanding of voice actors, harm the interests of vulnerable groups.

On balance, we hope that the PRAC³ framework, developed by a cross-disciplinary team, will increase awareness of the potential risks and harms faced by voice actors and benefit a wider range of stakeholders.

Positionality Statement

All authors are currently affiliated with US academic institutions, and all our interviewees also live in the United States. None of the team members identify as a member of the voice acting community. The research team includes members

who have long been engaged in risk and privacy security research, Human Computer Interaction, as well as members with extensive speech and audio technology research experience, which ensures that we are well-positioned to frame this research to understand the problems faced by voice actors from multiple perspectives.

Adverse Impact Statements

As the paper only contains non-experimental and non-identifiable interview data, we do not expect that the dissemination of this paper will have a substantial adverse impact. Our main concerns about adverse impacts are related to potential misunderstandings about the limitations of the research subjects, as described in the ethic statement.

References

A3MLAnticipatory. 2025. A3ML: Anticipatory and Adaptive Anti-Money Laundering. https://www.darpa.mil/research/programs/a3ml-anticipatory-adaptive. [Accessed 23-05-2025].

Acquisti, A.; John, L. K.; and Loewenstein, G. 2013. What is privacy worth? *The Journal of Legal Studies*, 42(2): 249–274.

Act, E. A. 2023. EU AI Act: first regulation on artificial intelligence — Topics — European Parliament — europarl.europa.eu. https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence. [Accessed 23-05-2025].

AESDD. 2018. Acted Emotional Speech Dynamic Database – AESDD. https://m3c.web.auth.gr/research/aesdd-speech-emotion-recognition/. [Accessed 27-01-2025].

Agnew, W.; Barnett, J.; Chu, A.; Hong, R.; Feffer, M.; Netzorg, R.; Jiang, H. H.; Awumey, E.; and Das, S. 2024. Sound Check: Auditing Audio Datasets. *arXiv preprint arXiv:2410.13114*.

Aleksic, P. S.; and Katsaggelos, A. K. 2006. Audio-visual biometrics. *Proceedings of the IEEE*, 94(11): 2025–2044.

Allen, A. L. 1999. Privacy-as-data control: Conceptual, practical, and moral limits of the paradigm. *Conn. L. Rev.*, 32: 861.

Allyn, B. 2023. 'New York Times' sues ChatGPT creator OpenAI, Microsoft, for copyright infringement. https://www.npr.org/2023/12/27/1221821750/new-york-times-sues-chatgpt-openai-microsoft-for-copyright-infringement. [Accessed 22-05-2025].

Andalibi, N.; Ozturk, P.; and Forte, A. 2017. Sensitive self-disclosures, responses, and social support on Instagram: The case of# depression. In *Proceedings of the 2017 ACM conference on computer supported cooperative work and social computing*, 1485–1500.

Ardila, R.; Branson, M.; Davis, K.; Henretty, M.; Kohler, M.; Meyer, J.; Morais, R.; Saunders, L.; Tyers, F. M.; and Weber, G. 2019. Common voice: A massively-multilingual speech corpus. *arXiv preprint arXiv:1912.06670*.

Baroni, M.; Bernardini, S.; Ferraresi, A.; and Zanchetta, E. 2009. The WaCky wide web: a collection of very large linguistically processed web-crawled corpora. *Language resources and evaluation*, 43: 209–226.

Bateman, J. 2020. Deepfakes and Synthetic Media in the Financial System: Assessing Threat Scenarios. Technical report, Carnegie Endowment for International Peace.

Baumgartner, J.; Zannettou, S.; Keegan, B.; Squire, M.; and Blackburn, J. 2020. The pushshift reddit dataset. In *Proceedings of the international AAAI conference on web and social media*, volume 14, 830–839.

BBC. 2021. Actor sues TikTok for using her voice in viral tool. https://www.bbc.com/news/technology-57063087. [Accessed 23-05-2025].

Blaising, A.; and Dabbish, L. 2022. Managing the transition to online freelance platforms: self-directed socialization. *Proceedings of the ACM on Human-Computer Interaction*, 6(CSCW2): 1–26.

Bloomberg. 2024. youtube says openai training sora with its video would break rules. https://www.bloomberg.com/news/articles/2024-04-04/youtube-says-openai-training-sora-with-its-videos-would-break-the-rules?sref=10lNAhZ9&embedded-checkout=true. [Accessed 22-05-2025].

CCM, C. 2024. CSA Cloud Control Matrix (CCM v4). [Accessed 27-01-2025].

Chakrabarty, T.; Padmakumar, V.; Brahman, F.; and Muresan, S. 2024. Creativity Support in the Age of Large Language Models: An Empirical Study Involving Professional Writers. In *Proceedings of the 16th Conference on Creativity & Cognition*, 132–155.

Cho, W. 2024. YouTube Creators Step Into Legal Battle Against OpenAI With Class Action Lawsuit. https://www.hollywoodreporter.com/business/business-news/youtube-creators-step-legal-battle-against-openai-class-action-lawsuit-1235968822/. [Accessed 23-05-2025].

Clarke, V.; and Braun, V. 2017. Thematic analysis. *The journal of positive psychology*, 12(3): 297–298.

Code; and Culture. 2024. The 3 C's of Voice Acting in the Age of AI: Consent, Control & Compensation. https://cultureandcode.io/gilfry-interview/. [Accessed 23-05-2025].

Communications, I. 2024. IATSE welcomes release of bipartisan U.S. Senate roadmap for AI policy, urges Congressional action - IATSE — iatse.net. https://iatse.net/iatse-welcomes-release-of-bipartisan-u-s-senate-roadmap-for-ai-policy-urges-congressional-action/#:~:text=their%20work%20is%20used%C2%A0to%20train%2C,new%20works%20by%20AI%20systems. [Accessed 23-05-2025].

Cook, A. 2024. Illinois BIPA: A Litigation Nightmare for Employers. *UIC Law Review*, 57(2): 5.

Ekene Chuks-Okeke, B. L., Ade Adetunji. 2023. Voice actors and generative AI: Legal challenges and emerging protection. https://iapp.org/news/a/voice-actors-and-generative-ai-legal-challenges-and-emerging-protections. [Accessed 23-05-2025].

EU. 2015. Creating Value through Open Data. https://data.europa.eu/sites/default/files/edp_creating_value_through_open_data_0.pdf. [Accessed 22-05-2025].

Gao, H.; Zahedi, M.; Treude, C.; Rosenstock, S.; and Cheong, M. 2024. Documenting ethical considerations in open source ai models. In *Proceedings of the 18th ACM/IEEE International Symposium on Empirical Software Engineering and Measurement*, 177–188.

GDPR. 2024. GDPRPrivacy Impact Assessment. [Accessed 27-01-2025].

Gero, K. I.; Desai, M.; Schnitzler, C.; Eom, N.; Cushman, J.; and Glassman, E. L. 2025. Creative Writers' Attitudes on Writing as Training Data for Large Language Models. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*, 1–16.

Godard, B.; Schmidtke, J.; Cassiman, J.-J.; and Aymé, S. 2003. Data storage and DNA banking for biomedical research: informed consent, confidentiality, quality issues, ownership, return of benefits. A professional perspective. *European journal of human genetics*, 11(2): S88–S122.

Gray, M. L.; and Suri, S. 2019. *Ghost work: How to stop Silicon Valley from building a new global underclass*. Harper Business.

Hoffman, S. 2015. Citizen science: the law and ethics of public access to medical big data. *Berkeley Tech. LJ*, 30: 1741.

Hutiri, W.; Papakyriakopoulos, O.; and Xiang, A. 2024. Not my voice! a taxonomy of ethical and safety harms of speech generators. In *Proceedings of the 2024 ACM Conference on Fairness, Accountability, and Transparency*, 359–376.

Jasserand, C. 2024. Deceptive Deepfakes: Is the Law Coping with AI-Altered Representations of Ourselves? In *2024 International Conference of the Biometrics Special Interest Group (BIOSIG)*, 1–4. IEEE.

Kagan, O. 2020. CCPA Regulations: Are Audio Recordings Personal Information? https://dataprivacy.foxrothschild.com/2020/06/articles/california-consumer-privacy-act/ccpa-regulations-audio-recordings/. [Accessed 23-05-2025].

Kang, D.; Hashimoto, T.; Stoica, I.; and Sun, Y. 2022. Zkimg: Attested images via zero-knowledge proofs to fight disinformation. *arXiv preprint arXiv:2211.04775*.

Kastrenakes, J. 2021. TikTok settles lawsuit with actress over its original text-to-speech voice. https://www.theverge.com/2021/9/29/22701167/bev-standing-tiktok-lawsuit-settles-text-to-speech-voice. [Accessed 22-05-2025].

Kaushik, S.; Sharma, T.; Yu, Y.; Ali, A. F.; Wang, Y.; and Zou, Y. 2024. Cross-Country Examination of People's Experience with Targeted Advertising on Social Media. In *Extended Abstracts of the CHI Conference on Human Factors in Computing Systems*, 1–10.

Kearns, J. 2014. Librivox: Free public domain audiobooks. *Reference Reviews*, 28(1): 7–8.

Kyi, L.; Mahuli, A.; Silberman, M. S.; Binns, R.; Zhao, J.; and Biega, A. J. 2025. Governance of Generative AI in Creative Work: Consent, Credit, Compensation, and Beyond. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*, 1–16.

Lane, J.; Stodden, V.; Bender, S.; and Nissenbaum, H. 2014. *Privacy, big data, and the public good: Frameworks for engagement*. Cambridge University Press.

Lee, J.; and Hong, I. B. 2016. Predicting positive user responses to social media advertising: The roles of emotional appeal, informativeness, and creativity. *International Journal of Information Management*, 36(3): 360–373.

Lefkovitz, N.; and Boeckl, K. 2020. NIST Privacy Framework: An Overview.

Liang, C.; Peng, J.; Li, Z.; and Yin, M. 2024. The valuation paradox of generative AI: Evidence from gig workers. *Available at SSRN 4825716*.

License, G. G. P. 1989. Gnu general public license. *Retrieved December*, 25: 2014.

Lin, T.-Y.; Maire, M.; Belongie, S.; Hays, J.; Perona, P.; Ramanan, D.; Dollár, P.; and Zitnick, C. L. 2014. Microsoft coco: Common objects in context. In *European conference on computer vision*, 740–755. Springer.

Liu, Y.; Chen, S.; Cheng, H.; Yu, M.; Ran, X.; Mo, A.; Tang, Y.; and Huang, Y. 2024. How ai processing delays foster creativity: Exploring research question co-creation with an llm-based agent. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*, 1–25.

Massiceti, D.; Zintgraf, L.; Bronskill, J.; Theodorou, L.; Harris, M. T.; Cutrell, E.; Morrison, C.; Hofmann, K.; and Stumpf, S. 2021. Orbit: A real-world few-shot dataset for teachable object recognition. In *Proceedings of the IEEE/CVF International Conference on Computer Vision*, 10818–10828.

Miller, P.; Styles, R.; and Heath, T. 2008. Open data commons, a license for open data. *LDOW*, 369.

Nagano, Y. 2025. California Creatives Rally Behind State AI Rules to Save Their Artwork. https://www.sfpublicpress.org/california-creatives-rally-behind-state-ai-rules-to-save-their-artwork. [Accessed 23-05-2025].

Nissenbaum, H. 2004. Privacy as contextual integrity. *Wash. L. Rev.*, 79: 119.

on Health Sciences Policy, B.; and on Strategies for Responsible Sharing of Clinical Trial Data, C. 2015. Sharing clinical trial data: maximizing benefits, minimizing risk.

OpenAI. 2025. How ChatGPT and our foundation models are developed. https://help.openai.com/en/articles/7842364-how-chatgpt-and-our-foundation-models-are-developed. [Accessed 23-05-2025].

Panayotov, V.; Chen, G.; Povey, D.; and Khudanpur, S. 2015. Librispeech: an asr corpus based on public domain audio books. In *2015 IEEE international conference on acoustics, speech and signal processing (ICASSP)*, 5206–5210. IEEE.

Pantiukhov, P.; Koriakov, D.; Petrova, T.; Alves, J. H.; Gurbani, V. K.; and State, R. 2024. Enhanced DeFi Security on

XRPL with Zero-Knowledge Proofs and Speaker Verification. In *2024 IEEE International Conference and Expo on Real Time Communications at IIT (RTC)*, 23–30. IEEE.

Prahallad, K. 2010. *Automatic building of synthetic voices from audio books*. Carnegie Mellon University.

Prahallad, K.; Raghavendra, E. V.; and Black, A. W. 2010a. Learning speaker-specific phrase breaks for text-to-speech systems. In *SSW*, 162–166.

Prahallad, K.; Raghavendra, E. V.; and Black, A. W. 2010b. Semi-supervised learning of acoustic driven prosodic phrase breaks for text-to-speech systems. In *Proceedings of 5th International Conference on Speech Prosody (Speech Prosody 2010), Chicago, Illinois*.

Purdy, G. 2010. ISO 31000: 2009—setting a new standard for risk management. *Risk Analysis: An International Journal*, 30(6): 881–886.

Romanosky, S.; and Acquisti, A. 2009. Privacy costs and personal data protection: Economic and legal perspectives. *Berkeley Tech. LJ*, 24: 1061.

Russakovsky, O.; Deng, J.; Su, H.; Krause, J.; Satheesh, S.; Ma, S.; Huang, Z.; Karpathy, A.; Khosla, A.; Bernstein, M.; et al. 2015. Imagenet large scale visual recognition challenge. *International journal of computer vision*, 115(3): 211–252.

Sambasivan, N.; Checkley, G.; Batool, A.; Ahmed, N.; Nemer, D.; Gaytán-Lugo, L. S.; Matthews, T.; Consolvo, S.; and Churchill, E. 2018. " Privacy is not for me, it's for those rich women": Performative Privacy Practices on Mobile Phones by Women in South Asia. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*, 127–142.

Schuhmann, C.; Beaumont, R.; Vencu, R.; Gordon, C.; Wightman, R.; Cherti, M.; Coombes, T.; Katta, A.; Mullis, C.; Wortsman, M.; et al. 2022. Laion-5b: An open large-scale dataset for training next generation image-text models. *Advances in Neural Information Processing Systems*, 35: 25278–25294.

Shan, S.; Cryan, J.; Wenger, E.; Zheng, H.; Hanocka, R.; and Zhao, B. Y. 2023. Glaze: Protecting artists from style mimicry by {Text-to-Image} models. In *32nd USENIX Security Symposium (USENIX Security 23)*, 2187–2204.

Sharma, T. 2024. Inclusive. AI: Towards Democratic AI with DAO-Enabled Inclusive Decision-Making. *OpenAI Grant Interim Report*.

Sharma, T.; Kaushik, S.; Yu, Y.; Ahmed, S. I.; and Wang, Y. 2023a. User perceptions and experiences of targeted ads on social media platforms: Learning from bangladesh and india. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, 1–15.

Sharma, T.; Kyi, L.; Wang, Y.; and Biega, A. J. 2024. " I'm not convinced that they don't collect more than is necessary":{User-Controlled} Data Minimization Design in Search Engines. In *33rd USENIX Security Symposium (USENIX Security 24)*, 2797–2812.

Sharma, T.; Potter, Y.; Kilhoffer, Z.; Huang, Y.; Song, D.; and Wang, Y. 2025. Aligning AI with Public Values: Deliberation and Decision-Making for Governing Multimodal LLMs in Political Video Analysis. *arXiv preprint*.

Sharma, T.; Stangl, A.; Zhang, L.; Tseng, Y.-Y.; Xu, I.; Findlater, L.; Gurari, D.; and Wang, Y. 2023b. Disability-first design and creation of a dataset showing private visual information collected with people who are blind. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, 1–15.

Tauberer, J. I. 2010. *Learning [voice]*. University of Pennsylvania.

Tenbarge, K. 2024. Scarlett Johansson says she was 'shocked, angered' when she heard OpenAI's voice that sounded like her. https://www.nbcnews.com/tech/tech-news/scarlett-johansson-shocked-angered-openai-voice-rcna153180. [Accessed 23-05-2025].

Thomee, B.; Shamma, D. A.; Friedland, G.; Elizalde, B.; Ni, K.; Poland, D.; Borth, D.; and Li, L.-J. 2016. Yfcc100m: The new data in multimedia research. *Communications of the ACM*, 59(2): 64–73.

Tseng, Y.-Y.; Sharma, T.; Zhang, L.; Stangl, A.; Findlater, L.; Wang, Y.; Tseng, D. G. Y.-Y.; and Gurari, D. 2024. BIV-Priv-Seg: Locating Private Content in Images Taken by People With Visual Impairments. *arXiv preprint arXiv:2407.18243*.

Van Horn, R. 2007. Online books and audiobooks. *Phi Delta Kappan*, 89(2): 154.

Yu, Y.; Sharma, T.; Hu, M.; Wang, J.; and Wang, Y. 2024. Exploring Parent-Child Perceptions on Safety in Generative AI: Concerns, Mitigation Strategies, and Design Implications. *arXiv preprint arXiv:2406.10461*.

Zarochintcev, S. 2021. Anticipatory Governance And National Security Risk Assessment. https://ideas.repec.org/a/nos/vgmu00/2021i3p200-218.html. [Accessed 23-05-2025].

Zhang, A.; Boltz, A.; Wang, C. W.; and Lee, M. K. 2022. Algorithmic management reimagined for workers and by workers: Centering worker well-being in gig work. In *Proceedings of the 2022 CHI conference on human factors in computing systems*, 1–20.

Zuboff, S. 2023. The age of surveillance capitalism. In *Social theory re-wired*, 203–213. Routledge.