(2) Does the increasing use or distribution of AI-generated material raise any unique issues for your sector or industry as compared to other copyright stakeholders?

The most unique issue AI-generated material raises in my industry are around media literacy and dis/misinformation. In a recent national survey, the grassroots organization Media Literacy Now reported that 25% of respondents were open to believing conspiracy theories.[1] The survey found that this was due to a combination of poor science literacy skills, social alienation, and heavy social media consumption patterns.

I am concerned that the general public does not know how to identify AI-generated images and that this can be taken advantage of *especially* on social media platforms given the deficits in public media literacy. Anecdotally, I often see others online share obviously AI-generated images as if they are not. Sometimes this is because the sharer didn't realize (to which AI watchdogs say "look at the hands!"[2]); other times (and more distressingly) the sharer knows the images are AI-generated, may have generated the images themselves, and genuinely *do not care* about any negative ramifications especially if they aren't the target. This latter type of sharer seems to only care about social media engagement metrics and social capital. To be clear, this is antisocial behavior that encourages deception, further erodes trust in the media, and makes it hard to tell fact from fiction.[3]

But I'm most worried about deepfakes, particularly with how quickly my own friends and family have adopted apps like Reface without any concern for how this same technology can be used for extremely malicious purposes. Deepfakes fall into what the Department of Homeland Security named "digital content forgery" in their *S&T Digital Forgeries Report* (2023). This is forgery that uses "emerging technologies, including artificial intelligence and machine learning techniques, to fabricate or manipulate audio, visual, or text content with the intent to mislead."[4] This type of forgery is often used for non-consensual pornography (also known as "revenge porn"), financial scams, and political misinformation; and it is a known threat.

(28) Should the law require AI-generated material to be labeled or otherwise publicly identified as being generated by AI? If so, in what context should the requirement apply and how should it work?

---

[1] https://reboot-foundation.org/research/science-fictions-low-science-knowledge-poor-critical-thinking-linked-to-conspiracy-beliefs/

[2] https://www.newyorker.com/culture/rabbit-holes/the-uncanny-failures-of-ai-generated-hands

[3] https://www.technologyreview.com/2019/10/10/132667/the-biggest-threat-of-deepfakes-isnt-the-deepfakes-themselves/

[4] https://www.dhs.gov/science-and-technology/publication/st-digital-forgeries-report-technology-landscape-threat-assessment

Because of the public's inability to discern AI-generated images from those not generated by AI, AI-generated images should be labeled as such — similarly to how the Federal Trade Commission requires social media influencers to disclose financial relationships with brands to their followers.[5] This would assist in public detection of deepfakes, and should be imperative for advertisements.

One instance where the labeling of an AI-generated image would have been helpful happened in June 2023, when a company named EstroLabs/QueerQuirk began advertising Hormone Replacement Therapy (HRT) supplements to transgender people on Twitter. Under closer scrutiny it became obvious that the company was a scam; Twitter users quickly realized that a picture of the company's "founder" was an AI-generated image of a Black queer person.[6] The use of Blackness, along with a generic "kicked-out for coming out" story, was most likely to give the fake company an air of legitimacy so it could collect transgender peoples' personal information more easily. In our current era of violent transphobia and legislation criminalizing gender affirming care, this type of AI enabled scam could have led to the harassment and doxxing of transgender people.

An ideal future copyright law should include clauses specific to digital copyright forgery, including deepfakes, and any intention to deceive the public and consumers. This could allow for those harmed by generative AI to seek legal recourse, though interpretation could privilege intent over impact. Because of this, future copyright law should also consider material harm and relational power (like media conglomerates suing artists with work for hire contracts[7]) as a counterbalance to intent.

(6) What kinds of copyright-protected training materials are used to train AI models, and how are those materials collected and curated?; (9) Should copyright owners have to affirmatively consent (opt in) to the use of their works for training materials, or should they be provided with the means to object (opt out)?

My major concern about training materials for AI models is data colonization —which is when major organizations and companies own and privatize citizens' and/or users' data.[8] Data colonization has dangerous implications regarding surveillance of the general public and directly undermines user consent. We are already seeing litigation for the misuse of data, especially user pictures and images.

---

[5] https://www.ftc.gov/business-guidance/resources/disclosures-101-social-media-influencers

[6] https://www.vice.com/en/article/z3mm88/a-sketchy-website-advertised-fake-hormone-pills-to-trans-people-then-it-disappeared

[7] https://www.reuters.com/legal/transactional/marvel-sues-comic-book-artists-over-rights-iron-man-spider-man-others-2021-09-24/

[8] https://harvardlawreview.org/blog/2023/06/data-colonialism-and-data-sets/

In 2022, the facial recognition platform Clearview AI settled in a lawsuit brought forth by the ACLU.[9] Clearview AI had scraped multiple social media platforms for billions of user pictures and sold the database to police departments, government agencies, and private groups. Users did not consent to their pictures being used in this way. In 2023, artists filed a class action lawsuit against Stability AI, Midjourney, and DeviantArt for copyright infringement.[10] And even established legacy companies are in the crosshairs — Getty Images also sued Stability AI in 2023 for using over 12 million of their photos as training materials without permission.[11]

There is a fundamental problem of consent with AI training models when they rely on forms of data colonization and mass scraping of data, and opt out models of consent are not adequate models of consent. Opt out models are presumptuous and place the burden on the public to even know that there is something to opt out of. Opt in models (affirmative yeses) and hybrid models would offer greater degrees of informed consent.

Generative AI disrupts our information ecosystem and complicates existing copyright law. Without careful consideration for how generative AI can be used maliciously, creators and the general public will continue to be harmed. To mitigate this, AI-generated images should be labeled as such, especially in the case of deepfakes and other models that can be used for digital content forgery. Training models also need to be created ethically, which includes informed consent. Without this, we will continue to see generative AI used in ways that oppose the purpose of copyright.

---

9 https://www.businessinsider.com/clearview-scraped-30-billion-images-facebook-police-facial-recogntion-database-2023-4

10 https://www.reuters.com/legal/transactional/lawsuits-accuse-ai-content-creators-misusing-copyrighted-work-2023-01-17/

11 https://www.reuters.com/legal/getty-images-lawsuit-says-stability-ai-misused-photos-train-ai-2023-02-06/